Managing Organizational Risk Using the Supplier Audit Program

Also available from ASQ Quality Press:

Advanced Quality Auditing: An Auditor's Review of Risk Management, Lean Improvement, and Data Analysis
Lance B. Coleman, Sr.

The Certified Supplier Quality Professional Handbook
Mark Allen Durivage, editor

The ASQ Auditing Handbook, Fourth Edition
J.P. Russell, editor

Proactive Supplier Management in the Medical Device Industry
James B. Shore and John A. Freije

The ASQ Supply Chain Management Primer
ASQ's Customer–Supplier Division and J.P. Russell, editor

Quality Risk Management in the FDA-Regulated Industry, Second Edition
José Rodríguez-Pérez

The ISO 9001:2015 Implementation Handbook: Using the Process Approach to Build a Quality Management System
Milton P. Dentch

The Certified Six Sigma Yellow Belt Handbook
Govindarajan Ramu

Handbook of Investigation and Effective CAPA Systems, Second Edition
José Rodríguez-Pérez

Practical Design of Experiments (DOE): A Guide for Optimizing Designs and Processes
Mark Allen Durivage

Quality Risk Management in the FDA-Regulated Industry
José Rodríguez-Pérez

The Certified Pharmaceutical GMP Professional Handbook, Second Edition
FDC Division and Mark Allen Durivage, editor

Failure Mode and Effect Analysis: FMEA from Theory to Execution, Second Edition
D. H. Stamatis

To request a complimentary catalog of ASQ Quality Press publications, call 800-248-1946, or visit our website at www.asq.org/quality-press.

Managing Organizational Risk Using the Supplier Audit Program

An Auditor's Guide Along the International Audit Trail

Lance B. Coleman, Sr.

ASQ Quality Press
Milwaukee, Wisconsin

American Society for Quality, Quality Press, Milwaukee 53203

Printed in the United States of America
24 23 22 21 20 19 18 5 4 3 2 1

Library of Congress Cataloging-in-Publication Data

Names: Coleman, Lance B., Sr., 1962– author.
Title: Managing organizational risk using the supplier audit program : an auditor's guide along the international audit trail / Lance B. Coleman, Sr.
Description: Milwaukee, Wisconsin : ASQ Quality Press, [2018] | Includes bibliographical references and index.
Identifiers: LCCN 2018006191 | ISBN 9780873899680 (hard cover : alk. paper)
Subjects: LCSH: Materials management. | Risk management. | Auditing, Internal.
Classification: LCC TS161 .C595 2018 | DDC 658.7—dc23
LC record available at https://lccn.loc.gov/2018006191

ISBN: 978-0-87389-968-0

Ray Zielke: Director, Quality Press and Programs
Paul Daniel O'Mara: Managing Editor
Randall L. Benson: Sr. Creative Services Specialist

ASQ Mission: The American Society for Quality advances individual, organizational, and community excellence worldwide through learning, quality improvement, and knowledge exchange.

Attention Bookstores, Wholesalers, Schools, and Corporations: ASQ Quality Press books, video, audio, and software are available at quantity discounts with bulk purchases for business, educational, or instructional use. For information, please contact ASQ Quality Press at 800-248-1946, or write to ASQ Quality Press, P.O. Box 3005, Milwaukee, WI 53201-3005.

To place orders or to request ASQ membership information, call 800-248-1946. Visit our website at http://www.asq.org/quality-press.

Printed on acid-free paper

Quality Press
600 N. Plankinton Ave.
Milwaukee, WI 53203-2914
E-mail: authors@asq.org
The Global Voice of Quality®

This book is, first and foremost, dedicated to my beautiful wife of over 31 years, Lorraine. You graciously put up with all the foibles inherent in living with a continuously improving, lean thinking, quality engineering, comic book reading, auditor-for-life kind of husband. You remain both my love and my inspiration. Next, to the newest addition to our family, my wonderful grandson Sheldon Kenneth Johnson Jr. Truly, the best is yet to come. I also want to dedicate this book to my children from birth—Larissa, Lauren, Lance Jr., and Latrice—as well as to my adoptive children, Sheldon Sr. and Veronica. A parent's greatest wish is for happy, healthy children that have an expanded worldview, with the potential to do more and to be *more. You, my children, have granted me that blessing. And last, but not least, I dedicate this book to my two dogs, Leo and Shii, for always making my return home a cause for celebration, even on the worst of days.*

(This page intentionally left blank)

Table of Contents

Part II: Supporting Skills

List of Figures and Tables

Preface

Risk elimination. Risk management. Risk mitigation. These terms are an increasingly important part of the lexicon of executive-level management as they strive to succeed in a business environment having global competition, geographically diverse suppliers, and new technologies. In this new, globally expansive marketplace, more than 50 percent of value creation is achieved outside of an organization's walls, or, in other words, through their suppliers. This, too, is where the majority of product realization risk lies. This book will help clearly define what risk-based thinking is and how to apply it from the perspective of helping manage organizational risk through the supplier audit process. Suppliers are increasingly global in nature, which makes understanding cultural nuance more important than ever in building successful customer–supplier relationships. The chapter on international auditing will provide a comparison between conducting domestic and international audits, as well as an understanding of how to successfully incorporate cultural understanding into supplier audit planning and execution.

Read on to learn how a robust supplier audit program can help manage organizational risk, and what role supplier audits *should* play in the supplier approval process. Join our discussion on conducting a successful supplier audit and how to identify, assess, and mitigate risk in the work environment. Auditing tips, tools, and techniques, along with practical application of various risk assessment tools, will be shared. You will also learn how to conduct a risk-based supplier audit. Finally, readers will learn how the incorporation of various improvement and quality tools into the audit process can produce results that will also minimize organizational risk while helping to optimize organizational performance. For those transitioning from first-party to second-party auditing, the difference between supplier and internal auditing will be explored. A glossary of important auditing terms is also included.

The book is divided into two sections plus a conclusion and appendix. The first section explores supplier management, supplier auditing, and the supplier audit process. The second section discusses the skills, both traditional and nontraditional, needed to ensure a successful supplier audit. Relevant aspects of the ASQ Certified Quality Auditor and Certified Supplier Quality Professional bodies of knowledge will be discussed in detail. Individual chapters contain relevant quotations, highlight key thoughts to understand, and share cases in point that illustrate important themes while providing tips on how to handle the various unusual situations that an auditor might come across when conducting supplier audits anywhere throughout the world.

Finally, I am thrilled to have friends and colleagues from around the globe sharing their own stories in conjunction with mine in crafting the "Case in Point" vignettes interspersed throughout the book. Thanks to them, some of the industries reflected within these pages include medical device, logistics, automotive, and aerospace. Tales from Canada, Kenya, and throughout the United States are included. This book is meant to provide a detailed and useful discussion of the practical application of risk-based supplier auditing principles. It is also intended to be a primer for those new to the profession of supplier auditing, and to share tips and best practices that would benefit experienced auditors as well. These pages represent experience gained while conducting hundreds of domestic audits as well as audits conducted in six countries around the world over the course of a 20-plus-year career in auditing. I have tried to "leave nothing on the table." I hope that you enjoy reading this work as much as I have enjoyed writing it.

Acknowledgments

I would like to acknowledge my friends and colleagues James Metto, Kristen Wagner, Janet Bautista Smith, Denis Devos, Sheronda Jeffries, and Shauna Wilson for taking time out of their busy schedules to contribute to the cases in point shared in the following pages. I would also like to acknowledge my friend and colleague Duke Okes for his support, for many engaging conversations on the latest and greatest in auditing, as well as for our collaboration on the development of new and unique training materials on the very important topic of risk-based quality auditing. Also, thanks to my friend and Six Sigma mentor Jim Boblett, who is a constant resource when it comes to understanding Six Sigma tools, methods, and uses. Any mistakes that I may have made in discussing the application of these tools will certainly be due to my own stumbles in understanding. I have to give a nod to the ASQ Audit Division, which, for over 26 years, has been setting the standard and constantly raising the bar internationally for what it means to be considered a professional auditor and for what it means to conduct a good audit. I am proud to be a member of your leadership team. I would like to thank Alexa Druckmiller for providing her editorial skills to assist me in presenting as polished a work as possible to Quality Press for their consideration. Lastly, I would like to thank my managing editor, Paul O'Mara, for his shared vision and support of this project in addition to the editorial efforts of his team in partnering to craft what I hope you will agree is a very readable and value-added work.

(This page intentionally left blank)

Introduction

To understand how supplier audits can help manage organizational risk, you must first understand where the supplier auditing process fits within the overall supply chain management system. The American Production and Inventory Control Society (APICS) provides the following definitions of supply chain and supply chain management:

- *Supply chain*. The global network used to deliver products and services from raw materials to end customers through an engineered flow of information, physical distribution, and cash. (*APICS Dictionary*, 15th Edition)
- *Supply chain management.* The design, planning, execution, *control*, and *monitoring* of supply chain activities with the objective of creating net value, building a competitive infrastructure, leveraging worldwide logistics, synchronizing supply with demand, and measuring performance globally. (*APICS Dictionary*, 15th Edition)

Control and monitoring of suppliers is where said auditing comes in. Review and analysis of supplier audit results is an important part of driving improvement and managing risk.

Why is the control and monitoring of suppliers so important? Often, more than 50 percent of value creation is achieved outside of the walls of an organization. In fact, almost 100 percent of manufacturers here in the United States have at least one aspect of their finished product created outside of their walls. With this being the case, there is huge organizational risk existent within the supply chain that must be well managed. Weaknesses within the supply chain can lead to quality problems, delivery issues, or both. Recent industry trends have shown regulators enforcing greater control over suppliers by manufacturers for these reasons. If you require

further justification, look to the news. Over the course of the past five years there have been multiple instances where supply chain concerns have made international news. Here are several of the most notable examples:

- 2016: Samsung recall of its Galaxy Note 7 due to fires resulting from lithium-ion batteries sourced from a supplier that provided 60 percent of the batteries used.
- 2016: Toyota recalls over 23.1 million vehicles worldwide due to malfunctioning Takata airbag inflators, whose malfunction has been linked by authorities to over 16 deaths internationally.
- 2013: European horse meat scandal where certain products advertised as being beef contained up to 100 percent horse meat.
- 2012: Tsunami offshore of Japan that disrupted supply chains worldwide for months.

Supply chain risk can manifest itself in the form of compromised consumer safety, product liability, tarnished business reputation, or a combination of these. In these few cited examples, you see safety issues due to product failure, problems caused by mislabeling (horse meat is not harmful to humans), and delivery issues caused by a natural disaster.

A basic model of the supply chain system from the perspective of the finished goods manufacturer is shown in Figure I.1, depicting delivery of components and raw materials from suppliers, transformation into finished goods by the manufacturer, and delivery to the end user.

To demonstrate how a supply chain functions, the Council of Supply Chain Management Professionals (CSCMP) has developed the SCOR (supply chain operations reference) model, which divides the system into five phases, as shown in Figure I.2.

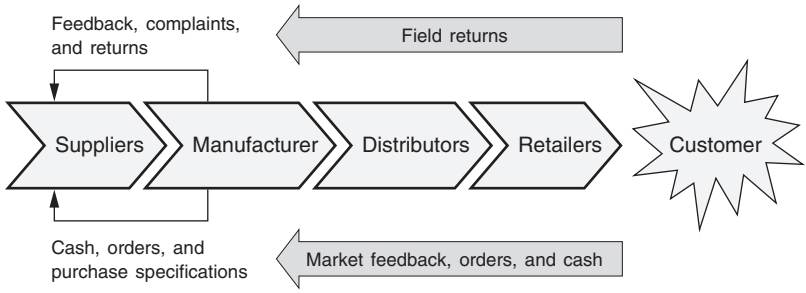


Figure I.1 Supply chain system model.

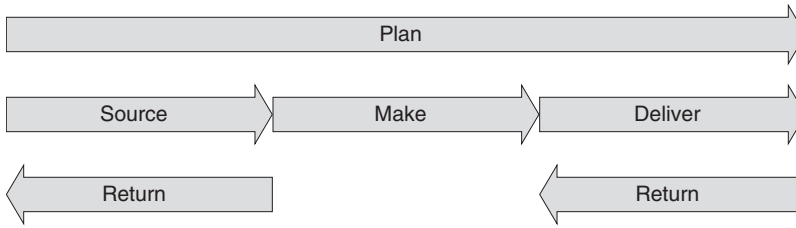


Figure I.2 SCOR model.

1. *Plan*. Planning to allow for balancing of supply with demand, communicated throughout the supply chain.
2. *Source*. The procurement of goods and services to meet demand. This includes identifying, selecting, and measuring performance of sources of supply, as well as delivering and receiving materials.
3. *Make*. Taking raw materials and components and transforming them into finished products having value for the end user.
4. *Deliver*. Providing resources to move materials along the supply chain from suppliers, to manufacturing, to customers. This includes order management, warehousing, and shipping.
5. *Return*. The reverse logistics process for product or material that is returned, including for repair, maintenance, and overhaul.

The ASQ Customer–Supplier Division body of knowledge (BoK) presents the *supplier life cycle management model* shown in Figure I.3. This model provides an integrated approach. It considers business and quality needs of the organization while also taking into account business and quality risks. Additionally, it is different from other models in that it explicitly considers reevaluation and decommissioning of suppliers as well.

The functional areas included within this definition of the supply chain system are information management, procurement, inventory flow scheduling and control, transportation systems and infrastructure, distribution facilities management, quality, and customer service (including order management and fulfillment).

As with other parts of a quality management system, supply chain management begins with the crafting of an organizational vision: What is our role in the marketplace? What are our values? Where do we see ourselves heading in the future? Blanchard and Stoner, from their 2011 book *Full Steam Ahead!*, identify three key elements of a compelling vision:

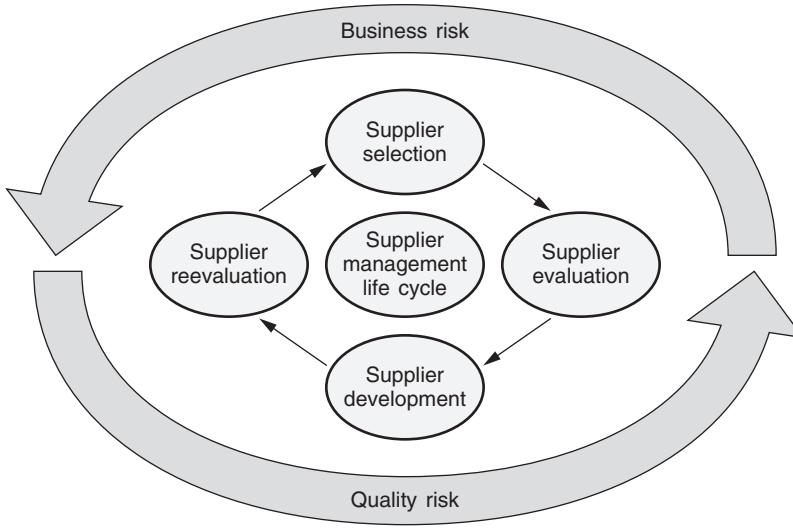


Figure I.3 Supplier life cycle management model.

1. Significant purpose
2. A picture of the future
3. Clear values

All three are needed to promote a common cause, clear and consistent direction, and motivation when times become difficult (and they will). From there, on a tactical level, a mission statement is developed that will support the strategic vision. Then strategies are developed that will allow for successful completion of the mission. That will break down silos and provide a road map for how organizational functions, such as information management, procurement, inventory flow scheduling and control, transportation systems and infrastructure, distribution facilities management, quality, and customer service, will collaboratively work together. Assuming the consistent requirement of a certain minimum level of quality, potential strategies that might be employed for supply chain management are low cost, quick turnaround/delivery, leading technology, compatible values, six sigma quality, or combinations of these and other factors. The strategies implemented will determine how risk tolerant the organization is. Operationally, suppliers would be selected, and then controls and monitoring put in place based on the overall strategy being deployed. Let us look at some examples:

- *Strategic vision*. Become a leading company worldwide; provide technologically advanced products that will help protect the environment.

  The sector that this company is working within is manufacturing and technology. They want to establish leadership in their market globally, not just nationally. Their corporate values relate to protection of the natural environment. They plan to use cutting-edge technology to achieve their goals.

- *Mission statement*. Establish mutually beneficial relationships with all suppliers, including those having new and unique products and technologies that will help this organization provide cutting-edge products that help preserve the environment.

  This is an example of what I call a "closed loop" mission statement. The first part of the mission statement pertains to the purpose of the supply chain management program, while the second half of the statement describes how this purpose supports the overall corporate vision. The benefit of this type of mission statement is that it "closes the loop" by prompting the organization to not just ensure that they are remaining on task, but to verify that successful implementation of the plan is moving the organization forward in the direction of the goals set by the organizational vision.

- *Strategy deployment*. Pursuing cutting-edge technology means that you are going to have to be more risk tolerant because new and, sometimes, unconventional suppliers may need to be included within the traditional mix. Additionally, new technology, while proven through validation and initial release, will not have the history of field data on which to base decisions, as would be the case with an established product.

  Controls, such as quality agreements, purchase specifications, surveys, audits, incoming inspection levels, performance triggers, and more, must take this increased risk into account.

It should be noted that supply chains exist both within and without an organization. Internal supply chains flow raw materials, components, and information through various processes, such as manufacturing, inspection, and testing, from the receiving to the shipping dock. They may consist of functions such as customer service, shipping and receiving, purchasing, production, and, finally, distribution to customers. Sound familiar? Another phrase for an internal supply chain is *value stream*.

There are three broad methods for assessing supplier capability (new) and performance (existing): surveys, audits, and sample inspection (AQL). The output of each of these processes is a *report*. Two important terms to be aware of when evaluating suppliers are *capability* and *capacity*:

- *Capability* is the ability to produce product that consistently and predictably meets requirements.
- *Capacity* is the ability to meet customer demand *and* the agility to ramp up to meet increased future demand as required.

Onboarding (setting up) a supplier is part of the control process. The following are typical risk-related questions to be considered when onboarding a supplier:

- Do we have a history with this supplier?
- Does this supplier need to be audited?
- Does this supplier require an on-site or desk audit or both?
- How often should this supplier be audited?
- Should scheduled audits be on-site or desk audits or both?
- What is the AQL for this supplier's product?
- How do we monitor and analyze supplier performance?
- What is our action trigger?

Supplier performance monitoring expectations should be communicated to the supplier up front and should consider both tangible and intangible factors. It should also be noted that, while risk is attached to both, it could be more easily overlooked when considering intangibles.

Tangibles:

- Quality
- On-time delivery
- In-full delivery
- Audit results
- Supplier corrective action requests issued

Intangibles:

- Easy to work with

- Responsive to questions or concerns
- Open and forthcoming with information

The examples that I have provided for both supplier onboarding and performance monitoring are meant to be exemplary rather than exhaustive. As you see, though, the supplier audit process is an important part of both supplier control and monitoring. Factors such as audit type, audit frequency, and audit team complement are derived using fact-based decisions driven by risk. So far, we have talked about supply chain management and how the supplier audit program can help manage risk that is inherent within a supply chain. Let us now discuss what, exactly, we mean by *risk*.

ISO 31000:2009 speaks to enterprise (business) risk and is meant to be applied across industries, in businesses of all sizes and types. ISO 31000:2009 defines *risk* as the effects of uncertainty on objectives. ISO 9001:2015 *Quality management systems—Requirements* defines *risk* as the effect of uncertainty. *Uncertainty* is as good a definition as any for risk. When you are uncertain, it is often because you lack knowledge. When you lack knowledge, there is a higher likelihood of failure when embarking upon a particular project or endeavor. Though risk can be defined many ways, depending on the source, it is consistently noted that risk has two primary components: the potential impact of an adverse event and the likelihood that the adverse event will occur. Risk, when realized, can negatively impact the consumer, the product, the business, or society as a whole. We will have a more detailed discussion on risk, risk management, and risk-based thinking in later chapters.

Proper classification of the supplier is crucial to determining the type and level of controls placed on them. One method of classification, cited in ASQ's *Certified Supplier Quality Professional Handbook*, is the *portfolio segmentation model* shown in Figure I.4, created by Peter Kraljic. Kraljic uses a two-by-two matrix as a means of placing suppliers into broad risk-based categories that allow an organization to institute similar controls on groups of suppliers based on the matrix quadrant that they fall within.

Kraljic's four broad categories of classification are listed below with an explanation of where and why they would fit on the matrix. Kraljic recommends the following purchasing approaches for each of the four product quadrants. So, where an organization places a supplier on the matrix will guide the purchasing strategy for that supplier.

1. *Strategic products (high profit impact, high supply risk)*. High risk and high reward—these products deserve the most attention from purchasing managers. Options include developing long-term supply relationships, regularly analyzing and managing risks,

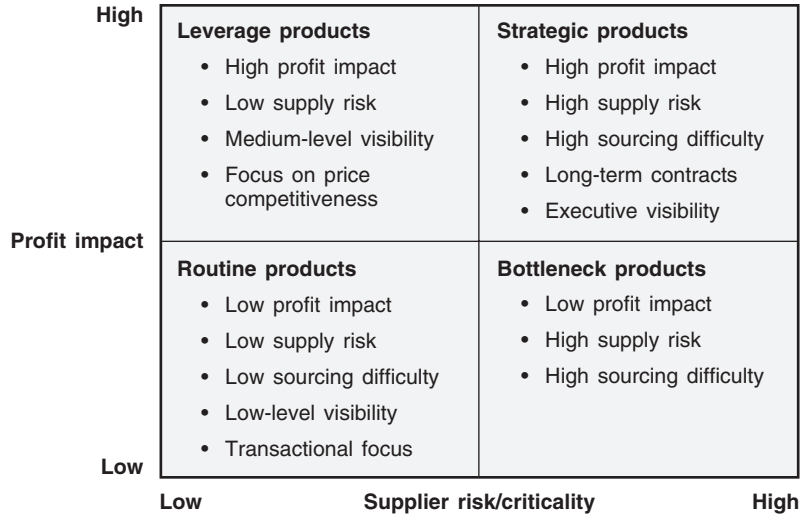


Figure I.4 Peter Kraljic's adapted portfolio segmentation model.

planning for contingencies, and producing the item in-house rather than buying it, if appropriate.

2. *Leverage products (high profit impact, low supply risk)*. Purchasing approaches to consider here include using full purchasing power, developing alternative products or suppliers, and placing high-volume orders.
3. *Bottleneck products (low profit impact, high supply risk)*. Useful approaches here include over-ordering when the item is available (lack of reliable availability is one of the most common reasons that supply is unreliable) and looking for ways to control vendors.
4. *Routine products (low impact, low supply risk)*. Purchasing approaches for these items include using standardized products, monitoring and/or optimizing order volume, and optimizing inventory levels.

Now that we have covered the basics of supply chain management and understand supply chain risk, we will answer the question "What exactly do we mean by *audit* anyway?" Two regularly cited definitions across industries are:

- Systematic, independent, and documented process for obtaining *objective evidence* and evaluating it objectively to determine the extent to which the *audit criteria* are fulfilled. (ISO 19011:2018)
- A systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled. (*The ASQ Auditing Handbook*, Fourth Edition)

Philosophically, the supplier audit function is a vehicle for assessing whether or not an organization is meeting its obligations, both stated and implied. It should serve principally as a focusing lens on areas of nonconformity, but also as a compass for mutually beneficial continuous improvement and risk management efforts. Operationally, the purpose of the supplier audit function should be determined by the supply chain management strategy as a reflection of company or site needs, goals, and objectives.

The purpose of a supplier audit is to confirm three general things:

1. Continued (or assessed if new supplier) ability to meet product requirements
2. Continued (or assessed if new supplier) ability to meet production demands
3. Maintenance of an effective quality management system

Before we move on, it is important to point out that supplier auditing is not just about confirming compliance, or managing risk, or even improving performance. When done well, supplier auditing is also about building supplier relationships. Creating a positive relationship between the customer and supplier helps ensure that the product will be fit for use, with minimal corrective action and inspection needed. According to Joseph M. Juran, there are nine primary activities needed to achieve this goal:

1. Define product and program quality requirements
2. Evaluate alternative suppliers
3. Select suppliers
4. Conduct joint quality planning
5. Cooperate with the supplier during the execution of the contract
6. Obtain proof of conformance to requirements

7. Certify qualified suppliers
8. Conduct quality improvement programs as required
9. Create and use supplier quality ratings

Upon reflection, you will note that each of these nine primary activities requires aspects of planning, clear communication, relationship building, and risk management in order to be successfully realized. Looking ahead, we will begin to discuss in detail how the supplier audit program helps manage organizational risk, as well as the nuts and bolts of supplier auditing, in the next two chapters.

Part I

Supplier Auditing and the Supplier Audit Program

(This page intentionally left blank)

Chapter 1

Managing Organizational Risk Using the Supplier Audit Program

Planning for the supplier audit program begins with goal setting, which flows down from the organizational vision and corresponding mission statement. Goals for the supplier audit program should be set in order to (1) meet required metrics, (2) align with the corporate vision and related strategies, and (3) help drive continual improvement (both organizationally and within the supplier audit program itself). Goals should follow the SMART principle—specific, measurable, attainable, realistic, time-based.

The organizational vision, mission statement, and context of the organization within its chosen market all help determine how risk tolerant an organization will be. For example, an established company that is working within a mature market has plans to grow its market share through economies of scale and incremental improvements. Such a company would likely be more risk averse than a company looking to employ cutting-edge technology within its product and processes as a key differentiator.

Examples of key risk-related questions to address during the supplier audit program planning are:

- How is risk managed overall?
- How do we define risk?
- Is risk management well integrated into our supply chain business processes?
- What are the risks and rewards in going with a sole or single-source supplier?
- How do we incorporate risk management into audit planning?
- How do we look at audit results from the perspective of risk?

- Is our risk management strategy aligned with the organizational vision and mission?

A balance must be struck between risk tolerance and resource constraints. Do we have the resources to successfully implement our chosen strategy? Do we need to gather more resources or modify the strategy?

Some common controls that might be put in place based on supplier risk are quality agreements (quality assurance), quality management system audits (quality assurance), technological review (engineering), and financial/business overview (supply chain), as well as receiving inspection protocols (quality control) and performance monitoring (quality assurance/supply chain). You can see even by this partial listing that proper planning for supplier control is a cross-functional effort. It is also important to note that even those aspects of the control system that go into effect after suppliers have been brought online should be determined during the planning process.

What is the auditing philosophy of our organization? The context of the organization within its marketplace is often, and should be, a key driver in developing the audit philosophy. Operating with either new or mature technology, or within a mature or emerging market, will be determining factors. Remember that one definition of risk is "the effect of uncertainty." So, embracing the uncertainty of entering new markets and utilizing new technologies can lead to higher risk and should precipitate tighter controls, among which supplier audits would be included. Branding as best quality or best economics will be a determining factor regarding when to do supplier audits, as well as what type of audits will be conducted. What resources are available, both financial and personnel, to support the supplier audit program? The answers to these and other related questions will then allow the organization to structure the supplier audit program in answering these tactical-level questions:

- Are on-site audits a last resort until high risk dictates otherwise?
- Are on-site audits a given unless low risk dictates? A decision tree such as shown in Figure 1.1 can be developed and used to help make this determination in most cases. In those instances that still are not clear, a discussion between quality, supply chain, and key interested parties should be held to make a final determination.
- How prominent is the supplier audit program among the different supplier controls (receiving inspection and test protocols, quality agreements, supplier corrective action requests, and so on) that have been put in place? See the relationship between supplier audits and

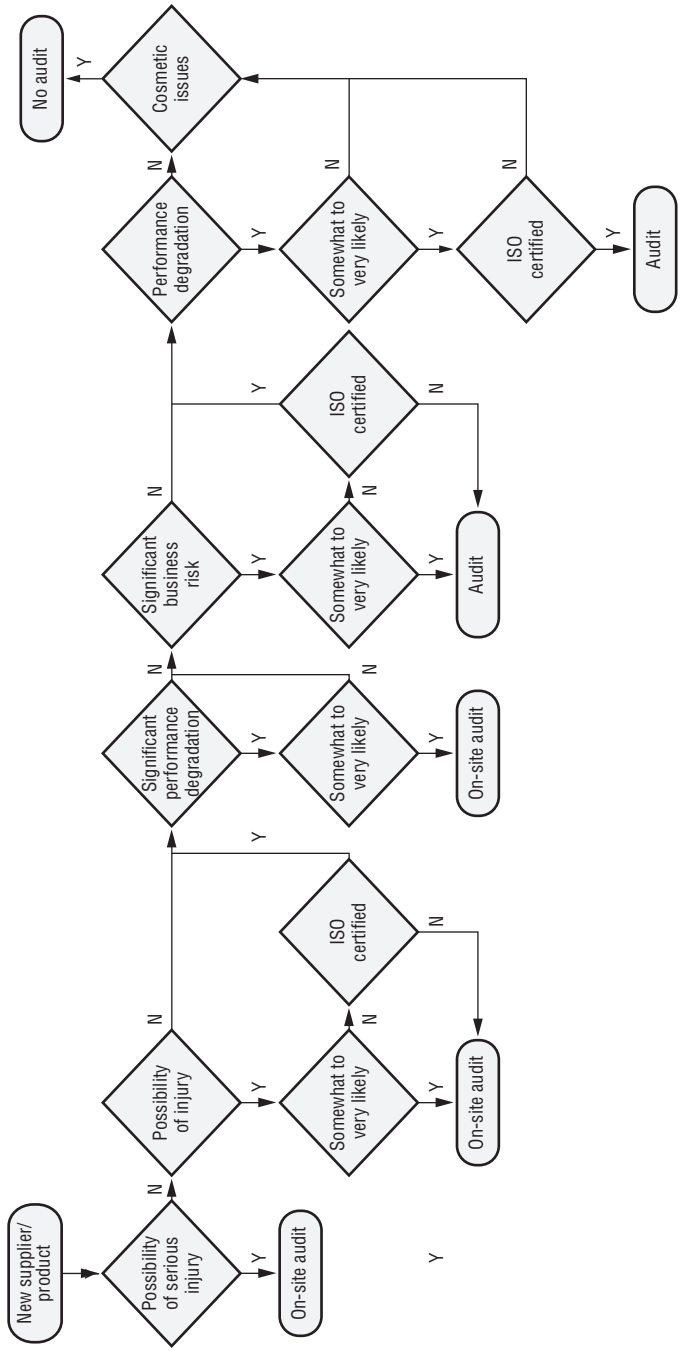


Figure 1.1 Supplier auditing decision tree.

other controls within the supplier management process in Figure 1.2.

It needs to be understood how we maintain a sightline with our organizational vision and build continual improvement into the DNA of our supplier audit program so that it helps drive us toward our desired future state. Another important factor for consideration is the development of standard work (practices). What technology platform (Excel, Word, iAuditor application, and so forth) do we use to generate audit working papers and otherwise support the supplier audit program? What types of audits will you do—system, process, product, element, or a combination of these, as appropriate? Are subject matter experts (SMEs) to be part of the audit team, meaning they would receive training as auditors? Or conversely, are SMEs primarily a support function with regard to the audit process, having a very specific role similar to administration or translation? Is our standard (default complement) one- or two-person audit teams? The consistency in both practice and appearance that comes with having standard work promotes efficiency and helps lend credibility to the audit program.

It is crucial to understand and clearly define the roles and responsibilities of the customer and supplier within the business relationship: who owns which responsibilities, and which, if any, responsibilities are shared? Ideally, there should be a baseline understanding or template(s) that can serve as a starting point for all quality agreements, but that can be built upon or revised as necessary to be specific to each supplier and the products that they provide.

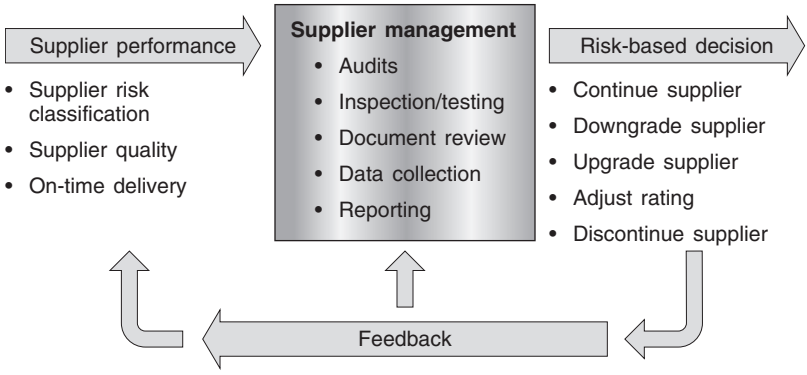


Figure 1.2 Supplier management process.

Supplier audit program planning needs to take into account three key elements—classification, response, and record keeping:

- *Classification*. Will you classify suppliers based on the highest risk of the products supplied—potential consumer risk, scarcity of the product they provide, business vulnerability, or some weighted combination of these factors?
- *Response.* What are the different levels of control that you put in place based on supplier classification? How are controls different during supplier setup and during performance monitoring of existing suppliers for the different classifications? What are our action triggers?
- *Record keeping.* What type of metrics should be tracked, which records should be kept, what medium should they be kept in, and for how long?

A periodic review of supplier audit program results against desired outcomes should be planned in order to determine acceptability of performance and whether or not goals need to be adjusted. Quantifiable metrics must be established to ensure a clear understanding among all interested parties as to what success looks like—both for the supplier and for the supplier audit program. It is important to sort this out beforehand because some supplier metrics and how you interpret them can be subjective. There is a very human tendency, when a supplier evaluation falls into the gray area of borderline evaluations, where the result is to take the "path of least resistance" and say, "this is okay." Notice that I *did not* say the "path of least risk." Having a clear understanding beforehand of what is and is not acceptable performance, in addition to what other factors should be considered in borderline cases, will help prevent this tendency to green-light a supplier that may require further reflection.

Two major pitfalls to avoid when planning the supplier management program are:

1. Going forward when there is a product that a company is desperate to have while there are quality management system, on-time delivery, financial, or other risks that would prompt a company with a mature quality management system to go forward only if they could put mitigations in place that would lower overall risks to an acceptable level. There is a reason, after all, that financial stability and business and quality systems, along with technical capability, are consistent considerations in evaluating suppliers. A mature organization might also try to form a relationship with

the supplier, if the supplier were willing, to help them develop to the point where the customer organization needs them to be. Otherwise, they would pass. No matter how desirable a new product or technology is, do not move forward with a supplier relationship unless you can mitigate any risks associated with the product, technology, or the supplier itself to an acceptable level.

2. Not having up front as clear as possible evaluation criteria as well as a structured and collaborative process for approving/disapproving suppliers that receive a marginal evaluation. Otherwise, unintentional bias may creep in for those suppliers that you "*really*, *really* want to use," for one reason or another, so that they are approved when they shouldn't be. This could mean having additional controls for suppliers receiving marginal evaluations, outright rejection of such suppliers, or some other response. How potential suppliers of important goods who have marginal evaluations are approved, disproved, onboarded, monitored, and controlled, shouldn't be left to chance.

Now let's look at how we develop an annual audit schedule. There are two principal things to take into account: needs and resources. For this scenario, let us assume that only high- and moderate-risk suppliers are audited, that low-risk suppliers are accepted based on ISO quality management system certification by an accepted registrar, and all suppliers must have an ISO quality management system certification.

First, ask your auditors the maximum number of audit days each is available for the year to determine the resources available. Plan for contingencies; take 90 percent of that number as your starting point. For example, you have 10 auditors and they can each give you six days per year. You have a total of 60 possible audit days. If you take 90 percent of that, you have 54 audit days. If we assume two days per audit, this allows for up to 27 audits with one auditor. If you wish to schedule two auditors per audit, you are now down to 13 possible audits, based on available resources. In actuality, the availability will vary from auditor to auditor, but for the sake of this example we will assume that all auditors have the same availability.

The next step is to look at the past three years and determine the average number of new supplier audits conducted. Let's say that number is four. You then have to set aside four audits to be determined (TBD) for the expected number of new supplier audits, which will leave you with the capacity to conduct nine planned audits of existing suppliers with your available resources. Following this process gives us a good sense of our capacity to conduct audits under optimal circumstances.

Separately, you have to determine which suppliers need to be audited based on risk and organizational procedures. First, you must identify which suppliers are due to be audited during the upcoming year as part of their (three-year, four-year, five-year, and so forth) cyclical rotation. Next, look at performance over the past year to see if any suppliers warrant being added to the schedule due to poor performance. This can be a first-time audit or possibly an audit that is moved up in the rotation to be performed a year (or more) early. Communicate with site management to inquire whether there are any suppliers that they may want to have audited for some other reason than poor performance (for example, considering them for new and/or different types of work).

Now that you know which suppliers need to be audited, you compare that with the number suggested by your available resources. If the need is greater than the resources, we can consider the following:

- Maybe two auditors aren't needed for every audit. If some audits have two auditors and some less complex audits only have one, we can increase the number of audits conducted.
- Remember that we identified resources based on 90 percent of maximum capacity. So, potentially, if everything goes as planned (and we know how often that happens), and we are able to audit at 100 percent of capacity, then that is another six possible audit days.
- Outside resources could be brought in, such as auditors from another company site, or contractors.
- Worst case, a determination could be made that there is low risk in pushing one or more audits back to the following year. This risk determination would likely be based on a combination of performance history and the product provided.

To go back to our example, let's say that 10 suppliers were due for auditing per their rotation, three suppliers need to be audited due to poor performance and inadequate response to supplier corrective action requests, and it is requested that two existing suppliers be added to the schedule because they are being considered to produce a very high-profile new component. All of this plus the four set-asides for new suppliers that need to be audited comprise the number of audits to be conducted. In this case we need to conduct 15 planned audits, while we have resources to conduct nine.

This reflects a shortfall of six audits or 12 audit days (six days auditing × two auditors per day). If we schedule at 100 percent of pledged capacity (60 audit days) instead of 90 percent, this gives us an additional six audit days. If we allow that six of the audits only require one auditor instead of

two as is standard, then that will give us another six audit days. This is not an optimal scenario since six of the audits will only have one auditor and because we have pushed our resources to the maximum. However, we have managed to close the gap between what must be scheduled and available resources to conduct supplier audits for the year.

Suppliers added to the schedule due to performance issues should be scheduled earlier in the year, followed by suppliers designated as high risk, then those designated as moderate risk. Next, those audits tied to projects, product development, or product release should be scheduled in time to provide the required information to those requesting the audit.

We should also consider the true worst-case scenario in which a company does not want to allocate funding or resources to conduct any audits. In that instance you will need to make the business case for the audit. Research nonconformance reports to determine scrap, rework, and processing costs (cost of poor quality [COPQ]) attributed to the worst-performing suppliers. Research any instances within the past three (arbitrary time frame) during which there may have been an instance where poor supplier performance cost the company money. Present this information to management along with your proposed audit schedule and projected costs. If you can make the case that spending $20,000 in costs to conduct supplier audits might prevent $50,000 in losses down the line, as evidenced by recent history, management may be more likely to approve at least some level of on-site supplier auditing.

So, here you have my guidelines for how to develop an annual supplier audit schedule. Take what works for you, adjust as you see fit, and leave out what you don't need. This audit development process as described is not meant to provide step-by-step instructions to account for every circumstance, but rather to provide you with a helpful overview of the thought process that you go through to put together an annual audit schedule, the questions that should be asked, and the things to be considered.

Auditing is, by its very nature, risk managing. Some of the ways that we plan for and respond to risk, both within the supplier audit program structure and within individual audits, are to determine:

- Audit frequency
- Audit length
- Audit type
- Audit team complement
  - Who is the lead auditor?
- How experienced should auditors be?

  - How many auditors?
  - SMEs required?
  - Translator required?
- Audit complexity ([Number of auditors × Number of days] + Level of sampling)
- Follow-up audits (needed or not)

Increased value comes by formalizing this process. The consistent application of risk-based thinking throughout all aspects of the supplier audit program, from planning through implementation, is key to successful mitigation of the risks that come from outsourcing. Wait a minute, hold up—risk-based thinking? What is that? Here is what ISO 9001:2015 says about risk-based thinking:

> *Risk-based thinking enables an organization to determine the factors that could cause its processes and its quality management system to deviate from the planned results, to put in place preventive controls to minimize negative effects and to make maximum use of opportunities as they arise.* (ISO 9001:2015, 0.1 General)

This is a pretty detailed and clear-cut definition of risk-based thinking, isn't it? Well, if you reread the paragraph above, you see that it is *not*. What this ISO standard excerpt is really talking about are the benefits of employing risk-based thinking. It does not say what risk-based thinking actually *is*. In fact, after reading through both ISO 9001:2015 and ISO 9000:2015 and searching the Internet, I was surprised that there was no precise definition for risk-based thinking found in any internationally recognized source. I could find the definitions of *risk* and *risk management*, but not risk-based thinking. I then referred to ISO 14971 and ISO 31000, where I again saw definitions for risk assessment, risk management, and many other related terms, but not risk-based thinking. Hmmm . . .

It looks like we will just have to come up with our own definition!

Risk-based thinking is a matter of perspective in how we view the data and situations that we encounter and respond to each day. As we know, a *process* can be thought of as an activity that transforms inputs into outputs—in this case, perceptions and data. So, risk management can be thought of as an output (response) resulting from the application of risk-based thinking to the data, observations, and activities (inputs) that we encounter every day in the workplace, as shown in Figure 1.3.

To understand how you would apply risk-based thinking to data analysis, let's look at a scenario where a company has 20 suppliers that should

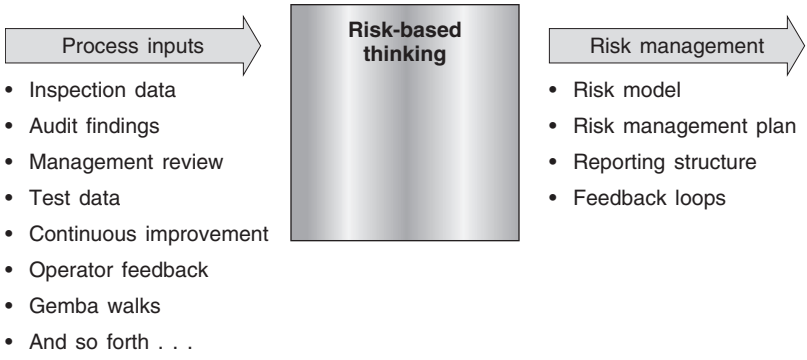


Figure 1.3 Risk-based thinking process map.

be audited this year according to the supplier auditing procedure, while only having resources to conduct twelve audits. You need to look at quality versus delivery and then process through multiple risk filters. Quality and on-time delivery (OTD) are selected for this scenario because they are the two most commonly used supplier performance metrics, in conjunction with other metrics. We will use a simple but effective prioritization tool to demonstrate risk-based thinking—the 2×2 matrix. You can put whatever you need to on the *x* and *y* axes in order to reflect the situation you are trying to understand. In this first case, we will place our suppliers A through T into a 2×2 matrix with quality on the *y*-axis and on-time delivery on the *x*-axis as shown in Figure 1.4. Once done, we see that we have four quadrants in the matrix reflecting the following conditions:

Quadrant I—No quality problems and no OTD problems

Quadrant II—No quality problems, but there are problems with OTD

Quadrant III—Quality problems and OTD problems

Quadrant IV—Quality problems but no OTD problems

The five suppliers in quadrant I are candidates to have their audits rescheduled. The five suppliers in quadrant III will definitely need to be audited. If a supplier is supposed to be audited per the long-range schedule and is having quality problems, then certainly they should be audited as well. Thus, the five suppliers in quadrant IV should also be added to the audit schedule. So, right now we have five audits that absolutely have to be done, five that should be done, and five that can be rescheduled.

Next we look at the five suppliers in quadrant II of Figure 1.4 with OTD issues but no quality problems. We place them on the 2×2 matrix (a business risk filter) seen in Figure 1.5. Do any of the suppliers provide product that if not available could affect customer delivery dates or multiple production lines? Looking at the matrix tells us that the two suppliers in quadrant III of Figure 1.5 pose a high business risk if parts become unavailable, so we add them to the audit schedule. The remaining three

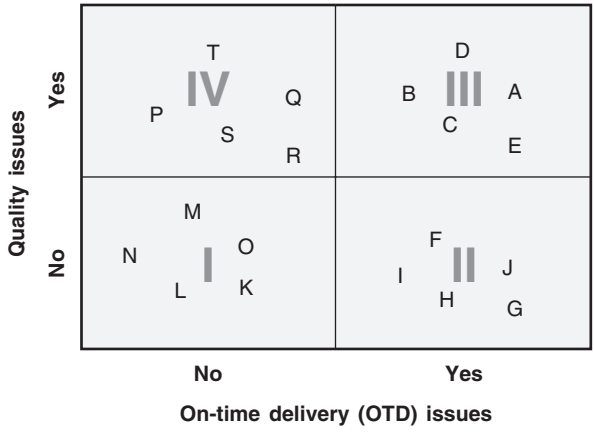


Figure 1.4 OTD issues versus quality issues.

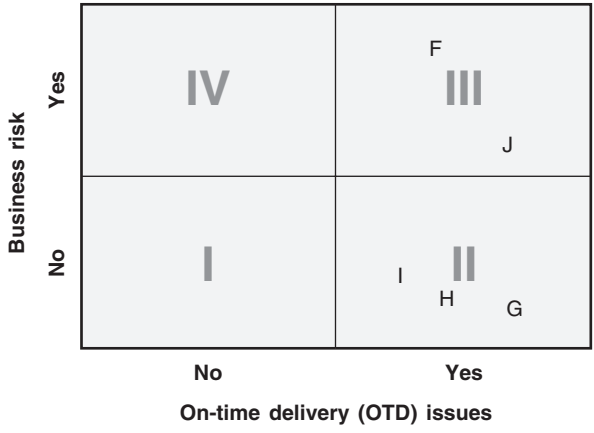


Figure 1.5 OTD issues versus business risk.

suppliers are candidates for rescheduling. The reason that I say *candidates* is that it is possible the company could acquire additional resources to close the resource gap that would allow them to audit all of the suppliers required within the year intended.

Now that we have arrived at a number of audits to be conducted that is in line with available resources, how would we prioritize them? First, those suppliers whose quality failures have either a 4 or 5 impact rating as defined in Table 1.1 should be prioritized. Then look at which failures have the highest *combined* impact and frequency of occurrence as defined in Tables 1.1 and 1.2. You will see in Table 1.3 the results of the prioritization.

To recap, we started out by considering how we might apply risk-based thinking to available supplier data pertaining to two key performance indicators—quality and on-time delivery. Then we reviewed the data through the lenses of consumer and business risk in order to make a fact-based decision on who to include on the audit schedule, and in what order they should be audited. Such a decision-making process helps the company manage risk and provides a defensible position when challenged by external auditors as to why certain suppliers were not audited as originally intended. It is very important to remember, however, that once it is demonstrated that there is low risk in rescheduling certain audits, the company must still demonstrate how they plan to recover. Otherwise, the same problem will reoccur the following year, now that eight scheduled supplier audits have been bumped back. This might mean converting some of the on-site audits for low-risk suppliers into desk audits (with justification), increasing available resources, or by some other means. If you are like me, then you rarely have all of the resources needed to accomplish *all* of the things you are tasked to do in the time allotted. That is why prioritization tools like 2×2 matrices are so helpful, particularly when applying risk-based thinking. Not only do they help visualize the data, but they also make a compelling statement, as opposed to a handwritten summary, when presenting your conclusions on whatever topic to management.

We just looked at applying risk-based thinking to supplier performance data. Now let's talk about how we might do the same with audit findings. Finding classification can be correlated to risk by combining the impact classifications as defined in Tables 1.1 and 1.2 with the frequency definitions shown in Table 1.3 for each audit finding; it is also possible by tying audit finding classification to risk level (see Table 1.4).

Another example of incorporating risk into finding classifications can be seen in Figure 1.6. In this instance, we use shading to designate the four levels of risk and then provide definitions for the four levels of impact and frequency that are combined to determine risk. The important thing to once again remember is that the levels of risk, the definitions, and even how

Table 1.1 Impact assessment.					
Impact	**1**	**2**	**3**	**4**	**5**
Definition	Improperly completed forms and records (information still retrievable)	Failure to meet requirements that do not impact fit, form, or function	Failure that could lead to issues with form, fit, or partial malfunction. Failure that could cause significant business risk	Failure that could lead to significant or total malfunction of end product	Noncompliance that is itself a hazard or may lead to hazardous conditions, or cause harm or injury

Table 1.2 Frequency of occurrence assessment.					
Occurrences	**1**	**2**	**3**	**4**	**5**
Definition	Fewer than 10% of lots or parts with issues	Between 10% and 20% of lots or parts with issues	Between 21% and 32% of lots or parts with issues	Between 33% and 50% of lots or parts with issues	Greater than 50% of lots or parts with issues

Table 1.3 Supplier audit priority list.

Priority	Supplier	Impact rating	Frequency rating	Overall risk rating
1	Supplier A	4	3	12
2	Supplier Q	5	1	5
3	Supplier P	4	2	8
4	Supplier C	3	4	12
5	Supplier F	3	4	12
6	Supplier D	3	3	9
7	Supplier E	3	3	9
8	Supplier J	2	4	8
9	Supplier T	3	2	6
10	Supplier S	2	2	4
11	Supplier R	2	2	4
12	Supplier B	3	1	3

Table 1.4 Risk level versus finding classification.

Risk	Finding classification
High	Major/critical
Medium	Minor/major
Low	Minor

risk is responded to should be defined in organizational procedures and be aligned with what has been determined appropriate by the organization.

Another method for taking risk into account when classifying audit findings is to assess the risk of failure against aspects of the quality management system based on the number and type of nonconformities identified within each area. For example, the sections of ISO 9001:2015 that would be assessed for risk are context of the organization, leadership, planning, support, operation, performance evaluation, and improvement. For a quality management system aligned with the Malcolm Baldrige framework, the aspects of the QMS assessed for risk would be leadership, strategy, customers, workforce, operations, results and measurements, analysis,

	Possible impact			
Frequency	**Negligible**	**Minor**	**Major**	**Critical**
Isolated incident				
Chronic				
Systemic				

Risk level	Finding classification
	Opportunity for improvement
	Minor noncompliance
	Major noncompliance
	Major noncompliance with need for intervention

Impact definitions	Frequency definitions
Negligible—An incident that has no product impact, an insignificant impact on operations, and, while it may be beneficial to improve, is not a violation of any kind.	*Isolated occasion*—One time or very infrequent occurrence. An occurrence that while possible, may never have occurred previously.
Minor—Violation of internal procedure or work instruction; Current practice that meets requirement is not accurately documented. Could lead to failure of part attributes. Isolated error.	*Chronic*—Issues or areas of concern that repeat over time. What is critical to understand is how often issues repeat and under what conditions.
Major—Violation of customer requirement or internal requirement. Systemic or chronic failure of QMS requirement. Multiple related minor viloations. Issue that could lead to failure of either finished good or part function or variables. Ethical violations. Issue that could cause great harm to other operations. Lost required record or procedure. Zero documented evidence of compliance. Direct violation of ISO standards or cGMP.	*Systemic*—Issues or areas of concern that repeat throughout different elements of the quality management or other organizational systems. Discovered during one time period over the course of a single audit.
Critical—Noncompliance that is itself a hazard or may lead to a hazardous condition. Issue that could directly lead to field failure of finished goods, potentially leading to injury of the end user. Legal violations.	

Figure 1.6 Finding classification risk matrix.

and knowledge management. Figure 1.7 shows examples of risk level classifications compared with aspects of the quality management system, based on audit findings.

In this case, it is not each individual audit finding that is assessed for risk, but rather the aggregate effect of all audit nonconformities related to a particular aspect of the quality management system and the risk of those nonconformities causing a failure in the system.

So, in thinking about how risk affects the classification of audit findings, we can look at the risk of individual nonconformities, the risk found within aspects of the quality management system, or the risk found within the overall quality management system (we can also directly audit the risk

Risk Level Definitions

A—Significant risk:

Potential for product contamination, complete product failure, or serious supply chain disruption.

Potential violation of customs/regulatory requirements or blatant disregard of technical/quality agreement.

Multiple systemic or chronic deviations from the requirements.

Conformity required within three months or according to agreement.

B—Moderate risk:

Required procedures do not exist, or exist but are not implemented or followed.

Lack of awareness or attention to cGMP requirements.

Lack of IT and other technical resources appropriate to the size of the business.

Deficient management systems for handling customer service, production planning, and inbound/outbound logistics.

Significant number of instances of partial fulfillment of requirements.

System is not achieving defined objectives.

Compliance required within six months or according to agreement.

C—Minor risk:

Regulatory, ISO, contractual, and internal requirements met in principle but not in full.

Current system needs additional focus and other improvements.

Compliance required within six months or according to agreement.

Figure 1.7 Risk level definitions for audit finding classification.

management program itself, as discussed in the next chapter). Finally, supplier audit program planning also takes into account risk when determining:

1. Audit frequency
2. Special training requirements for auditors
3. Complexity of individual audit plans
4. Minimum sample size required
5. Whether containment is necessary
6. The level of detail needed within corrective action plans
7. Effectiveness verification requirements

Thus far we have introduced the concepts of the supply chain and supply chain management. We have an understanding of how the supplier audit program responds to and helps manage risk. Now let's talk about what it means to conduct a risk-based supplier audit.

(This page intentionally left blank)

Chapter 2

Conducting a Successful Risk-Based Supplier Audit

Though our focus will be on risk-based supplier auditing, many of the tools and techniques discussed within this chapter would be beneficial in conducting any type of audit. As we will see below, the focus of a supplier audit can vary. Why, then, our emphasis on conducting risk-based supplier audits?

- *Compliance*. Do policies/procedures comply with requirements, and are they effectively implemented?
- *Performance*. Are desired/expected results being achieved by the QMS?
- *Risk*. What risks exist for which controls may not exist or be adequate? What risks are inherent to the quality management system?
- *Improvement*. What are some opportunities for improvement, and the risks associated with them?

When a supplier has a mature quality management system, it is unlikely that there will be major nonconformities. Management could begin wondering about the value of the audit program when only minor issues or opportunities are reported, becoming complacent and lessening support for quality initiatives. For the mature quality management system, the greatest opportunities will lie in managing risk to help drive improvement. Additionally, risk-based supplier auditing better protects the public (by helping manage risk), the customer, and the company as a whole. It leads to more-effective auditing and better management of limited resources, and makes for more efficient and effective processes. The four phases of any audit are planning, execution, reporting, and closure.

PLANNING

Now, before any audit planning can be done, authority to access the facility and conduct an audit must first be verified. This prevents wasting time in preparation for an audit that the supplier might not allow. Typically, the right to conduct audits is included within the contracts or quality agreements between supplier and customer. If this has not been done, an audit request can still be submitted to the supplier, but they will not be contractually obligated to comply. Two terms that are critically important in classifying the individual audit and that should be confirmed as the first steps in planning are:

- *Purpose*. The "what and why"—what are we doing, and why are we here? *Example:* "Confirm conformity of Supplier ABC quality management system to ISO 9001:2015 and Customer XYZ purchase specifications."
- *Scope*. The "where and when." *Example:* "The audit will take place at Supplier ABC in the Land of Oz on May 22, 2018, during first shift."

Along with confirming your authority to conduct the audit, the purpose and scope of the audit should be identified before any further audit planning takes place. A decision tree such as shown in Figure 2.1 can be used to help determine the audit team complement.

An important part of any audit, time management is even more critical when auditing suppliers. You typically don't get the chance to "come back to finish up" the next day. Managing your time during an audit starts with a well thought-out audit agenda. You will want to schedule a tour at the start of the audit in order to understand how work flows through the area(s) being audited. Limit the tour to 30 minutes, though. You don't want to take away too much time from the documented information review, interviews, and observations that take place during the rest of the audit. The rationale behind this practice is that during many supplier audits the audit team is only allowed to see processes in operation and records pertaining to product provided to the audit team organization. When possible, supplier audits should be scheduled when at least one of the auditing organization's processes is running, but this cannot always be accomplished. This may be due to the infrequency that certain jobs run, scheduling logistics, or lack of support from the supplier. When such is the case, you want to limit your tour to 30 minutes so that you can focus on audit evidence specific to your organization—records, documents, and overall quality management system effectiveness.

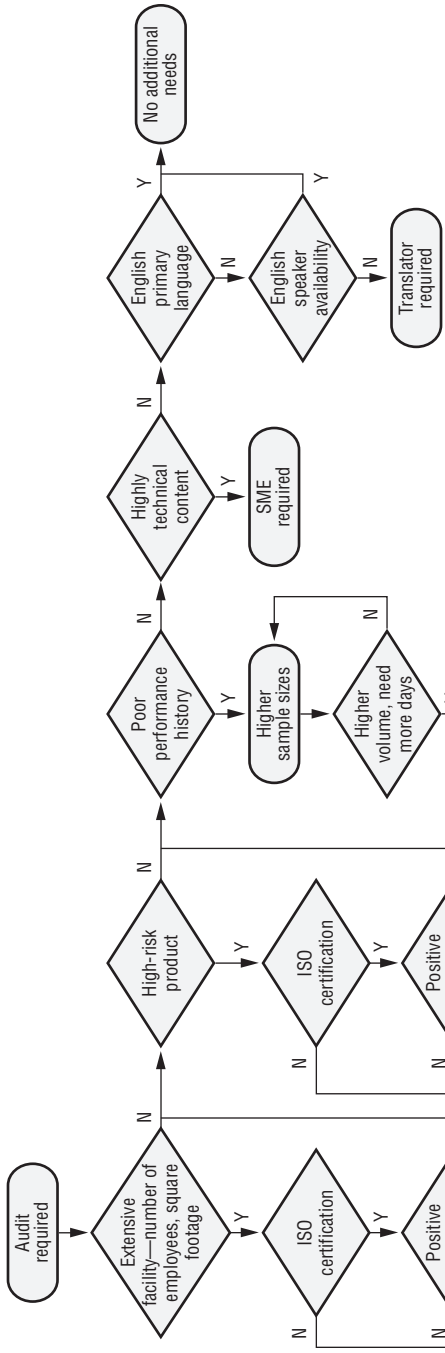


Figure 2.1 Audit team complement decision tree.

When you can arrange for one of your jobs to be running during the time of the audit, you can allow for up to 60 minutes for the tour in order to allow for time to ask more-detailed questions about the process and equipment where your job is running. Then you will want to schedule time to come back out on the floor later during the audit, possibly to conduct a process audit as part of the overall supplier audit. Plan to spend as much time as possible and as makes sense out on the floor where value is created. Having said that, it is important to find the balance that exists between being out on the floor observing, interviewing, and interacting with frontline employees and having enough time to thoroughly review relevant documents and records.

It is not necessary to follow the exact sequence of clauses of the criteria that you are auditing against on your schedule. However, you do want to start with an overview of the quality management system (for example, quality manual and quality policy) and leadership responsibility (leadership commitment, leadership communication, management review, and so forth). Then go over any nonconformities that need to be reviewed from the previous audit or any other items of concern (slipping performance, open supplier corrective action requests, for example). After that, organize the agenda in order to increase the likelihood of successfully reviewing all planned aspects of the quality management system. If there are areas where there often are no problems or that are easy and quick to review, move those toward the end of the schedule. That way if the audit team is running behind, they can either take smaller samples or perhaps skip a certain subclause with minimal risk of missing a significant nonconformance. Include an hour in the schedule before the closing meeting for audit team discussion and review of notes. This meeting is where the audit team reaches consensus on the classification of audit findings, and typically takes about a half hour. By scheduling an hour, you give yourself a 30-minute buffer that you can use if you are running behind. If the audit is on schedule, trust me, no supplier will complain if an audit ends 30 minutes early!

For an organization to function effectively, it needs to identify and manage numerous linked processes. The application of a system of processes within an organization—together with the identification and interactions of these processes, and their management to produce the desired outcome—is referred to by ISO quality management system standards as the "process approach." One important aspect of the process approach is conducting process audits. Now, how exactly do you conduct a process audit? The basics are pretty simple, actually:

- Confirm that all of the inputs are correct.
- Assess how the process is performing.
- Confirm that outputs are as expected.
- Compare output yields to other lines.

One example of how you would start a typical process audit would be to ask questions pertaining to the inputs based on the 6 M's—man, machine, material, method, measurement, and Mother Nature (environment):

- Man:
  - Operator knowledgeable of operation
  - Operator training records available
- Machine:
  - Equipment calibrated
  - Equipment maintained as required
  - Equipment correct
  - Settings correct
- Material:
  - Correct materials
  - Materials not defective
  - Required certificates (conformance, analysis, and so forth) available
- Method:
  - Operator actions match instructions
  - Instructions used are the most recent revisions
  - Instructions are correct
- Measurement:
  - Correct data being captured
  - Data capture done correctly

- Mother Nature:
  - Any environmental condition requirements met
  - Environment monitored
  - Safety and cleanliness evaluated
  - Line clearance effective

Next, you will assess how the process is performing and how it is being monitored:

- Performance:
  - Performing as expected
  - Gauge/meter readings as expected
- Monitoring:
  - Monitored as required
  - Data recorded as required
  - Data trending appropriately
  - Correct data being captured

Finally, a review of the outputs will take into account the following:

- Products:
  - Per specification
  - Yields as expected
  - Yields comparable to similar processes
- Records:
  - All required available
  - Completely filled out
  - Correctly filled out
- Signals:
  - Alerts, alarms, status signals sent as required
  - Sent alerts, alarms, and signals correct

- Consequences or risks associated with the overall process:
  - Properly mitigated

The type of process auditing where you follow the steps of a process from beginning through to the end is called *forward tracing*. An auditor could also start with the process outputs and work backwards. This method is referred to as *backward tracing*. You will notice in the process map in Figure 2.2 that one of the outputs of a process that should be considered is *risk*. Remember, for any activity that you are engaged in, there will always be some risks, however small. These could be risks of failure, injury, mistakes, and so forth. Now let's take a look at what happens when we shift the focus of the audit to risk.

How in-depth an audit is required to be depends on a combination of risk assessment, vulnerability of the organization, and performance history. Constraining factors are available resources and the level of accessibility to the supplier facility. The first step in planning for the audit is to determine what type of risk-based audit you wish to conduct. Risk-based quality audits can be thought of as having three levels:

- *Level 1*. Plan, audit, and report based on the risk found within each QMS process or within the QMS as a whole, as discussed in the previous chapter.
- *Level 2*. Evaluate the degree to which risk management is accomplished within QMS processes. To better understand the distinction between levels 1 and 2, risk-based audits let us look at the following scenario.

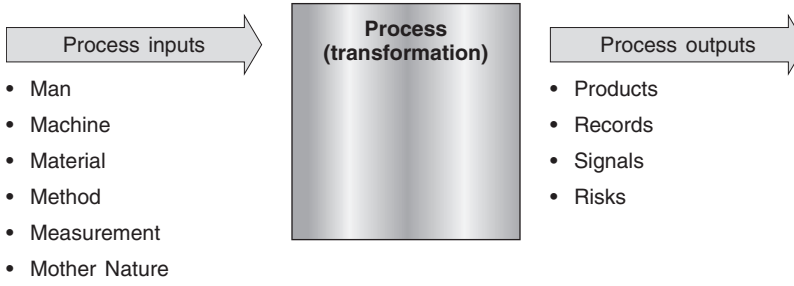


Figure 2.2 Process map.

Scenario: An auditor visits a machine shop and witnesses a welding operation where sparks are flying in the immediate vicinity. The operator is following their instructions and wearing the appropriate personal protective equipment (PPE), but the auditor notices a small puddle of oil on the floor nearby.

The hazards in this scenario are the sparks and the oil. The risks are those of slipping and falling, the sparks burning the worker, or the sparks catching the oil on fire. The key here is for the auditor to assess whether (1) all required controls (risk mitigations) are in place, and (2) whether they are adequate for the existing risks.

If the audit focus was on confirming conformity of this process, some of the questions to be asked might be:

- Is the operator performing the operation correctly?
- Do training records indicate that the operator has been trained on the latest revision of the relevant procedure?
- Do the parts being made meet requirements?
- Is equipment in the area calibrated and/or maintained as required?
- Are production records being properly completed and maintained?

If the audit focus was on performance or improvement, typical questions asked might be:

- Does the yield for this process meet expectations?
- How does the yield for the process compare across shifts, operators, work centers, and so forth?
- What opportunities for improvement are seen within the area?

An auditor might combine these different types of questions into one audit checklist where risk is a part of the evaluation, or do an audit where the sole focus is risk management, as opposed to level 1 risk-based supplier auditing where the focus is on verifying conformity and assessing the risk of quality management system failure, based on the identified nonconformities.

- *Level 3.* Determine enterprise- (business-) level risks related to QMS processes. In other words, based on the overall risks of failure

of the quality management system, is there risk of negative impact on other integrated business systems? Alternatively, at level 3 the risk management program itself is audited.

When auditing the risk management program itself, you should seek to verify all of the following:

1. The program should encompass all aspects of the product life cycle from design to end-of-life disposal.
2. Data from external, as well as internal, sources should be captured and analyzed, and the risk model should be updated as necessary.
3. Teams, when formed, should be cross-functional in nature in order to model the broadest range of risks.
4. Confirm that results from the risk management program are reported as necessary to appropriate levels of management.
5. Confirm that existing risk management procedures and work instructions are followed.
6. Ensure that organizational training supports the risk management program. Top management, middle management, engineering, and hourly workers may all require different levels of training. However, all levels of the organization should be trained to some extent in risk management.
7. Ensure that periodic review and assessment of the need for a risk model update is embedded within the risk management program.
8. Confirm that adequate resources are supplied to meet the goals of the risk management program.

Once the authority to conduct the audit, and the audit purpose and scope, are confirmed, then planning can begin in earnest. Overall planning for the audit is accomplished by the lead auditor and should, as a minimum, address the items below. When there is only one auditor on the team, then that person is by default the lead auditor.

1. Review audit purpose, scope, and previous audit reports.
2. Develop a plan:
   - What type of audit are you conducting?
   - Implementation strategy.

- Resources needed.
- Logistics to address.

3. Determine the number of audit days.
4. Review regulatory and other external websites for any issues on the public record.
5. Communicate within and without the organization to identify any known or suspected performance issues.
6. Prepare audit assignments.
7. Communicate/coordinate with audit team.
8. Communicate/coordinate with auditee.

Once the planning is done and audit dates are confirmed with the auditee and the audit team, we then transition to the execution phase of the audit. Sometimes this phase of the audit is referred to as "field work."

EXECUTION

While on the tour it is okay to ask occasional questions for clarification that can be answered easily during the tour. It is also okay to ask if you can jot down equipment numbers and material identification during the tour so that you won't have to come back out on the floor during the calibration or material traceability portions of the audit. However, don't linger too long in one area or begin asking complex questions. You will typically be on a tight schedule when conducting a supplier audit. Asking in-depth questions begins to turn the tour into an ad hoc audit within the audit, which can disrupt the audit plan flow and possibly the schedule timeline. This could lead to not having time to review an important area. Remember, you can always come back out as necessary. Again, the exception to this rule would be when product supplied to your company is running on the line while the audit is being conducted. The amount of time spent on the floor should also be reflective of the complexity of the processes being audited. As a very broad rule of thumb, spend up to 15% of your time on the floor when your job(s) are not running and up to 50% of your time on the floor when your job(s) are running. Typically, once you have verified that there is a controlled procedure for records maintenance, the actual maintenance of records can be confirmed using the records that are looked at throughout the day while reviewing various aspects of the quality management system.

The key to managing time effectively is to be as efficient with time as possible while at the supplier's site. Review the schedule each hour to

ensure that you remain on track and respond appropriately when you are falling behind. This may mean shifting assignments, reducing sample size, or even not auditing some aspect of the quality management system during the audit as planned. As a worst-case scenario, you could request certain records for review after you have left the site; keep this to a minimum, though, and understand that certain records will only be allowed to be reviewed while at the supplier's site.

The process approach espoused by the various ISO quality management system standards lends itself very well to managing risk. Before we dive in, though, let's review what we mean by a process. A *process* can be thought of as any activity that transforms inputs into outputs. In other words, some action has to be taking place; something has to be going on. A transformation also has to take place such that the items, materials, actions, methods, and so forth, that are put into the process are changed in some way and give something new and different as an output. Let's look again at the generic process map shown in Figure 2.2. In this instance, the possible inputs to a process are separated into the categories referred to as the 6 M's:

- *Man*. The actions taken by a human operator to initiate and/or facilitate the process.
- *Machine*. The equipment used during the process.
- *Material*. The raw material, components, and subassemblies that are going to be transformed.
- *Method*. The manner in which the operator is instructed to carry out their actions as indicated by standard operating procedures, work instructions, or through some other vehicle.
- *Measurement*. Any measurements or indicator readings that must be taken as part of the process.
- *Mother Nature*. The environment, such as any temperature, humidity, or cleanroom requirements; proper line clearance (all materials, documentation, and detritus from previous job removed from the work center); and lack of clutter in the area.

It has been found over time that most process inputs can be divided into these categories, though by no means is this the only way that you can classify inputs. Process inputs should be categorized according to what is most appropriate for the organization and the process under study. For outputs of a process, you have product (whether physical goods or some service), related documentation (completed forms/records), any identified process risks, and, when applicable, signals transmitted (that is, for computer or electronic systems).

To conduct a risk-based audit of a process, you will want to look at any risks inherent in the process inputs, the performance of the process itself, and the process outputs. Some of the risks that you would want to look for are the risks of nonconformity of raw materials and components, the process not performing as expected, operator error, test or inspection error, environmental issues, equipment failure, and so forth. In order to do that, you want to take the following steps:

1. Identify area hazards and risks.
2. Classify the hazards and risks.
3. Determine whether the risks are accounted for in the risk model.
4. Determine whether controls/risk mitigations are in place.
5. Determine whether controls/risk mitigations are adequate.

Scenario: A publishing company provides typographical services to their clients for the revision of their annual reports. The company job proposals include cost per hour and number of hours expected to complete the job based on the number of pages to be revised and the estimated number of changes per page. Runners deliver the work to work cells. Each work cell consists of two typists and two proofreaders, as shown in Figure 2.3. The process is as described below and shown in the process map in Figure 2.4, with inputs and outputs to each process step.

1. Individual pages are received with handwritten modifications.
2. Page recipient:

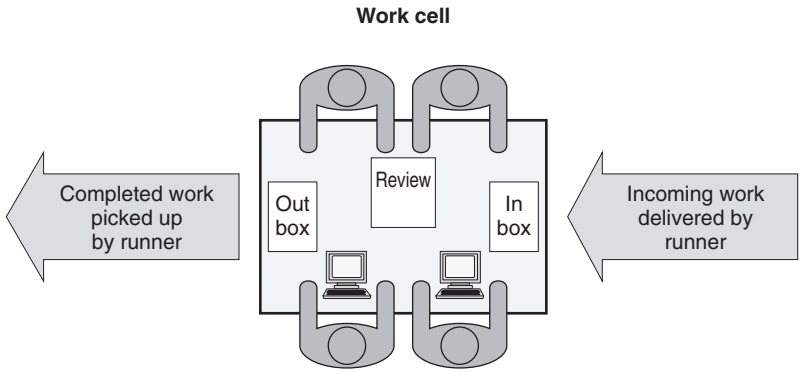


Figure 2.3 Publishing work cell.

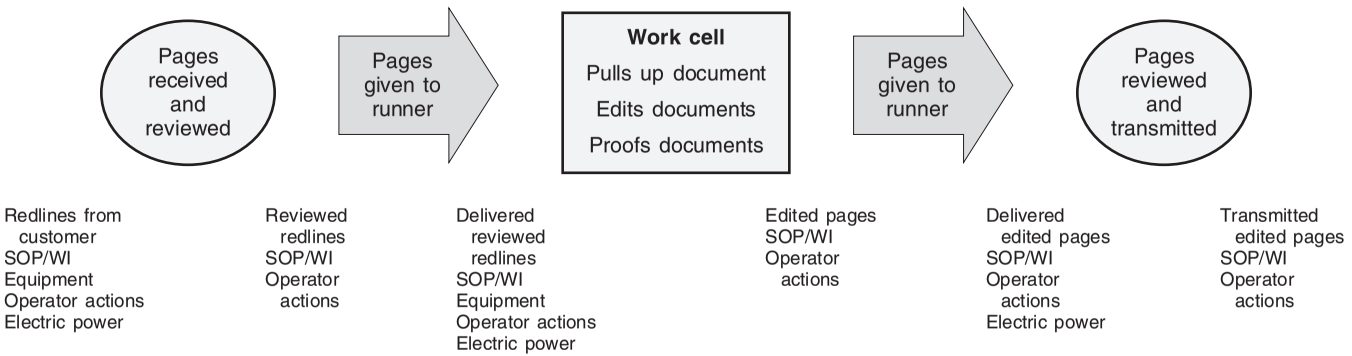


Figure 2.4 Document page revision process map.

   a. Verifies that the pages go to an active job
   b. Verifies that requested changes are legible
   c. Calls runner over and hands over pages for assigned work cell
3. Runner:
   a. Verifies which work cell pages go to
   b. Delivers pages to designated work cell in-box
4. Work cell:
   a. Typist:
      i. Pulls up document to be revised from SharePoint
      ii. Types in changes
      iii. Corrects any errors found by proofreader
   b. Proofreader:
      i. Proofs documents
      ii. Returns errors to typist for correction
      iii. Puts completed pages in work cell out-box
5. Runner:
   a. Picks up pages from work cell out-box
   b. Delivers pages to job planner
6. Job planner:
   a. Transmits document to customer

As you look at Figure 2.5 you will see that for every process step there are risks and hazards that could lead to either failure of that process step or failure of the overall process. Some are immediate while some are long term, but all should be addressed. Take note that for every hazard there is an associated risk, but the inverse is not true. You will also notice that the hazard of *poor lighting* is shared across each process step while the hazard of *old style keyboard* is only an issue within the work cell.

In Figure 2.6 you will see that various controls have been added to eliminate or mitigate certain risks and hazards. As an auditor, you will need to make an assessment when going through an area of whether or not controls are adequate to appropriately mitigate inherent process risks. You will

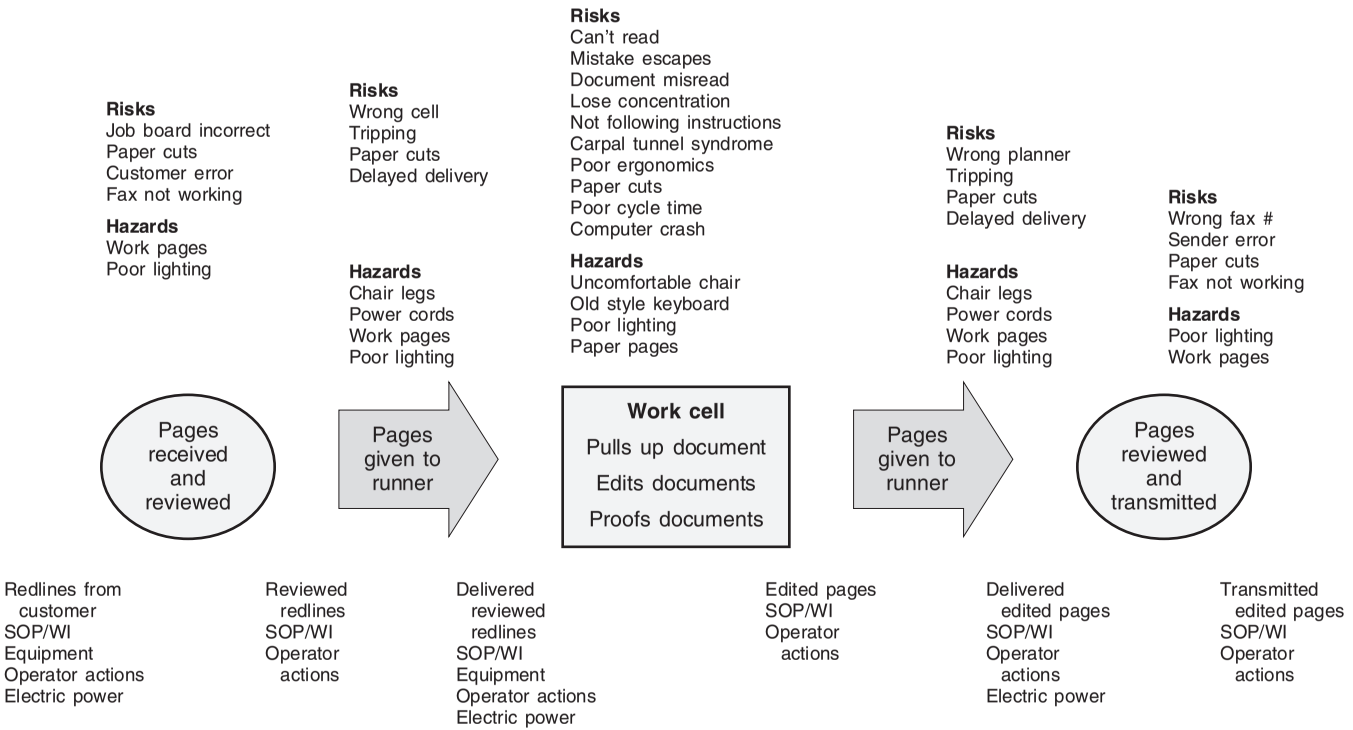


Figure 2.5 Document page revision process map showing hazards and risks.

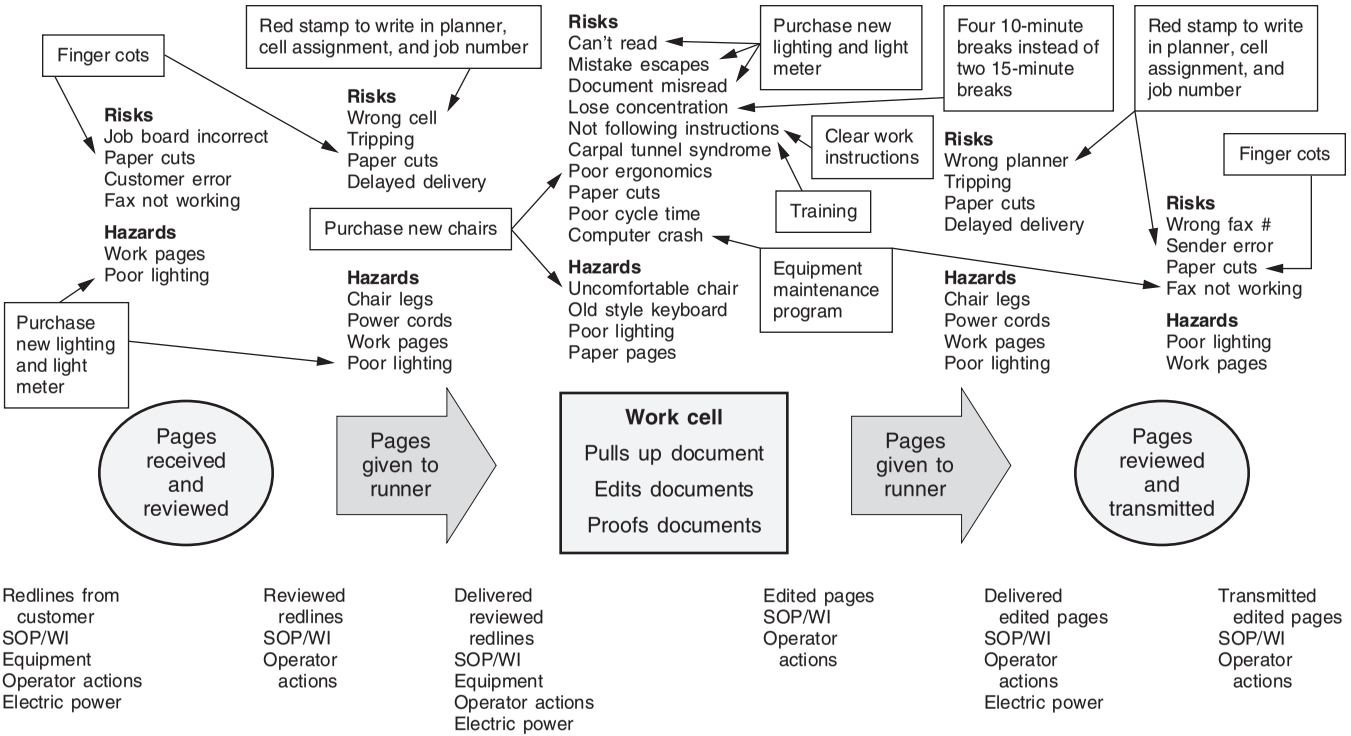


Figure 2.6 Document page revision process map showing hazards, risks, and controls.

also make a determination of whether there are any risks or hazards that have not been addressed. If so, then this may be considered either a nonconformity or opportunity for improvement based on the nature of the identified risks. How might you address the identified tripping hazard? What are some other risks/hazards that you see that should be addressed? How would you address those? If controls are found to be inadequate to address area risks, then this would be a nonconformity against the risk management program. If controls overall are adequate, but could be better, then these would be opportunities for improvement.

So what is the benefit of going through this type of exercise? When simply verifying compliance, there is a tendency to have "tunnel vision." "Procedures are being followed, training records are available, there are no 'red flags' jumping out at me, so we are good." However, an area can be conforming 100 percent to their procedure, but there may still be something important that was overlooked and is not addressed by the existing procedure. By opening their mind to try to identify every possible risk and hazard, and then assessing the controls in place to address each—of which the area standard operating procedure would be one—the auditor will often identify areas of concern that have been overlooked. The regulatory, ISO, and company requirements that preside over the area in question would then determine whether the oversight would be classified as either a nonconformity or opportunity for improvement. As stated earlier, this type of audit can be done as a stand-alone audit or as one aspect of a compliance or performance audit.

Note: For a more detailed description of this methodology across a more complex process map, look to the Risk Is the Compass model developed by Denis Devos in the 1980s and discussed briefly in my previous book, *Advanced Quality Auditing: An Auditor's Review of Risk Management, Lean Improvement, and Data Analysis.*

We have just taken the *process* approach to risk-based auditing. Now let's see how we would employ risk-based thinking when using the *elemental,* or *clause,* method of auditing.

When using the element method, the lead auditor should first assess the company documentation against the related clauses (elements) of the reference or external requirements. Any findings would then be against the supplier quality management system. Usually, this is done partially during a document audit that is part of the audit planning phase and partially on-site during audit execution.

Then auditors should compare employee actions and records (performance) against what is stated in their own internal documentation. Any findings noted would be against a lack of performance of actions as required. One way to think of this is that in step one you are validating that

the quality management system functions as required. In step two you are verifying that, given the appropriate inputs (flowed-down requirements and documentation), the outputs (actions and results) are as expected. This approach is called the "W factor" and is depicted visually in Figure 2.7.

When a nonconformity breaches both an internal and an external requirement, then write one finding against the internal requirement but reference the external requirement. In other words, pull an excerpt from the internal document as the requirement, state what was observed, and then draw your conclusion. Reference the external requirement document number and relevant clause but not any of the language from the external document. The reason you would cite only one nonconformity in this instance is because you don't want to "double dip." Even though two requirements were violated, there is only *one* nonconformity. The reason that you will quote from the internal document requirement is that it is likely to be more detailed, more relevant to the company, and provide more information than the external source. The reason that you still want to reference the external source is to prevent the auditee from just stating as a corrective action that "we decided we don't need to do that" and changing the procedure. See Figure 2.8 for an example.

Findings can be classified as minor, major, or critical according to the risk classification of the individual finding as shown in Chapter 1 and Table 1.2 and Figure 1.8. Risk may also be determined according to the potential cumulative effects of the findings relating to a specific area of the quality management system. In the instance cited in Figure 2.8, the risk would be minor since this was the only finding of nonconformity against the

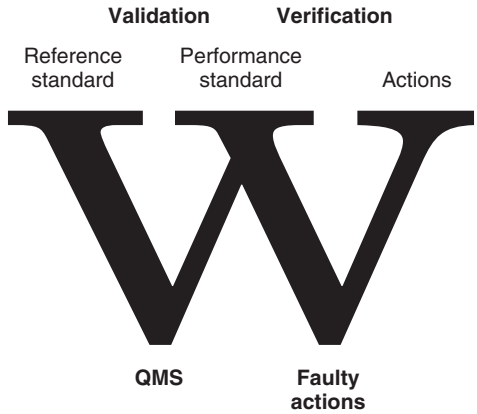


Figure 2.7 The "W" factor.
Source: Erik Myhrberg. Moorhill International. Used with permission.

Finding: AF-02	**Classification:** Minor noncompliance	**QMS reference:** Purchasing controls

Requirement:

PUR-001:5.3.1 (Revision D)—"Purchasing documents shall include, where possible, an agreement in which the suppliers, contractors, and consultants agree to notify the manufacturer of changes in the product or service so that manufacturers may determine whether the changes may affect the quality of a finished device." *External reference:* 21 CFR Part 820.50

What was observed:

- Purchase order supplier instructions do not include a requirement to inform supplier of any changes that may affect product quality.

Conclusion:

The requirements for purchasing controls are fulfilled in principle. This finding represents partial nonfulfillment of the requirement. Minor noncompliance.

Figure 2.8 Documentation of audit findings.

"purchasing controls" aspect of the quality management system. If chronic and/or systemic issues had been found, then the risk of failure of this aspect of the quality management system would have been elevated.

As mentioned previously, one key difference between supplier and internal audits is *transparency*. The vast majority of suppliers want to showcase their company and its processes, and so will be open and transparent. There are exceptions, however, when an auditor will receive intentionally misleading responses to their inquiries. There are also times when the data presented are suspect. Auditors need to recognize when this is the case. Studies have shown that we as humans communicate information following the pattern below:

- Body language 55%
- Vocal (tone) 38%
- Words 7%

Thus, it is key to not just hear *what* is being said but to listen for *how* it is being said. Also, look for any telltale body language cues. Two examples of behaviors to look out for when you believe there is information that an auditee representative may be intentionally hiding or misrepresenting are avoiding eye contact (though this could sometimes simply be a sign of nervousness) or changing behavior (for example, speaking louder, faster, or slower, looking away quickly before answering the question, faster blink rate than previously, and so forth). When you are unsure about a response, listen to your instincts and probe deeper. When reviewing reports and other

data, be sure that you understand what success looks like when represented in a report or on a graph. Don't just accept "pass" or "accept" on an inspection or test report. Don't just accept a series of plotted data points that appear to be acceptable based on the image. Determine what the acceptable value range is for a sampling of criteria and verify that that the actual numbers incorporated within the report or plotted on a graph are truly passing.

While conducting the audit, whatever type it may be, it is important to remember that supplier audits are not just about confirming that the supplier is meeting requirements. Supplier audits are also an important part of building relationships. Auditors must always remember that they are the guests of the auditee. As such, they are bound by auditee rules while in the area, and should not touch, review, or copy anything or speak with anyone without first asking permission. Auditors should be fair in their presentation, follow site rules, and engage with the auditee in a polite and nonpunitive manner. Any deviation from acceptable behavior runs the risk of alienating the auditee, ruining rapport, and making it difficult to acquire the information and support needed in order to conduct a successful audit.

The communication established during the audit is a two-way street. As a supplier auditor, you should also be receptive to identifying any gaps in desired behavior on the part of your organization. Does your organization respond to inquiries or approval requests in a timely fashion? Does your organization communicate drawing and specification changes in an effective and efficient manner? Are you reasonable in your requests? Don't forget to bring back opportunities for your organization to better help the supplier. If you do identify things that your organization can do better to help the supplier, don't just put it in your report and forget about it; follow up to see if the issue was addressed or at least assigned to someone to look into as an action item. Such behavior will promote greater transparency from the auditee, increasing the likelihood of a successful audit and improved relations.

KEY THOUGHT

An auditor should not allow themselves to be unescorted in a work area for more than a few minutes. Being unescorted for too long can open the auditor up to potential liability and other issues.

Even when you behave as the perfect guest, conflict will occasionally arise. In order to keep an audit on track, and to maintain access to required

information, conflicts must be resolved quickly and effectively. Conflicts can occur with the auditee or within the audit team itself. Conflict can be a significant risk to the successful completion of a supplier audit. There are different ways to handle conflict:

- *Avoiding* an issue or person is not an option if the conflict is relevant to the audit.
- *Smoothing over* may be an option if the issue is minor or irresolvable. Those in conflict should focus on what they agree on instead of what they don't agree on.
- *Forcing someone to accept or overpowering* someone is not good practice unless it is the only remaining option to ensure a successful audit.
- *Compromising* assumes that everyone can accept less than they originally asked for, resulting in no one getting exactly what they wanted.
- *Collaboration or problem solving* seeks to find a mutually agreeable solution to the conflict—a "win–win" scenario.

Collaboration is always the preferred method of handling conflict but must sometimes take a back seat to the realities of ensuring a successful audit. There will be times when the lead auditor has to listen to input from both sides of a disagreement and just "make the call."

REPORTING

Reporting of supplier audit results is fairly standard across industries and goes something like the following:

- *Quality management.* Every audit report
- *Supply chain management (and/or procurement).* Every audit report
- *Supplier.* Their audit report
- *Site management.* Supplier audit results summary report
- *Site management.* Supplier audit program evaluation report

Audit report distribution of risk-based quality audits, however, is a bit different because such audits and their results are more high profile. Due to the fact that risk management can address public safety and environmental pro-

tection, as well as business viability, there is much higher visibility at the director or vice president level for risk-based supplier audit reports. In fact, depending on the nature of the findings, the lead auditor would, in some cases, escalate report distribution to top management even when they wouldn't be on the normal report routing. A typical individual supplier audit report will include:

- Audit purpose and scope
- Audit criteria
- Lead auditor and audit team members
- Summary of results
- Result details, including identified risks
- Audit finding definitions and explanations
- Review of findings (nonconformities, opportunities for improvement, and positive practices)
- Review of corrective actions
- Identification of the need (or not) for a follow-up audit
- Opportunities to improve for *your* organization

The risk-based individual supplier audit report will also address:

- Identified supplier risks and their assessments
- Risk mitigations
- Residual risks
- Any risks attached to how *your* organization conducts business with the supplier

A summary of supplier audit results, along with an assessment of supplier audit program effectiveness, should be presented during the formal management review required by ISO quality management system standards. This should also include, at times as indicated by organizational procedure, those organizations whose quality management systems are ISO conforming. For those organizations who are not ISO certified and who do not claim conformity, the summary of supplier audit results and supplier audit program assessment should be delivered to top management as directed solely by organizational procedure. Following are typical topics that would be addressed within the supplier audit results summary report:

- Summary statement of conclusions based on the data presented
- Any assumptions made in drawing conclusions
- Trending and coding
- Any risks identified by trending of data that should be addressed
- Results of any mitigations put in place based on the previous meeting
- Assessment of the supplier audit program against previously established performance metrics
- Review of findings over time
- Review of causes

The summary of supplier audit results should then be used as an input for both the continual improvement and risk management processes by upper management.

CLOSURE

The expectations for audit closure are also based on risk. Generally, audit closure occurs upon reaching one of four conditions:

- Upon distribution of report (only when no nonconformities)
- Upon acceptable response to report and proof of implementation of accepted corrective action
- Upon presentation of evidence of successful effectiveness verification of the corrective action identified in the accepted response (best practice)
- Upon successful conclusion of a follow-up audit (when due to the number or severity of nonconformities, risk dictates that a follow-up audit is required)

AUDITING "HACKS"

- Once you have developed a checklist, or other audit working papers, that works well and gives you good results, turn it into a template. This will serve as a reminder of what to review when

next auditing the related area or function. This will promote greater consistency between audits and auditors. It will also establish a minimum bar for what is to be accomplished during a particular audit. I say "minimum bar" because it is important not to let templates and preprepared checklists handcuff you as an auditor. Each audit is different, and we as auditors should always look to see how we can improve on the practice of previous audits. Thus, while a valuable tool, established templates and "canned" checklists should be the beginning of audit preparation, not the end result.

- This "hack" is related to the first one. When you have a well thought-out audit form, type in the information while you are conducting the audit. This may slow you down somewhat, however, the closing meeting report-out will be much easier because you won't have to comb though pages of notes in order to identify and list your findings in an easy-to-present manner. Also, we know that our other duties will likely start pulling at us as soon as we return to our home sites. This often distracts from or detracts from the time needed for the final steps necessary to complete, submit for review, and distribute the audit report. By typing as much information into the form as possible while on-site at the supplier, you will find that the time needed to generate and distribute the audit report once you return to your home site will often be more than cut in half
- If auditing is your profession, begin to build your own library of standards. It is incredibly convenient to have files that you can easily refer to on your own computer when you wish clarification on specific requirements. Most companies have a subscription to those ISO standards that are relevant to them, which employees can access. Download them to your work computer. If you leave one company to go to another, check the standards library of your new employer first thing for what standards there are that you need to add to your new work computer. Sometimes, when attending a paid training you will be given a copy of a standard as part of the materials. In that case, you can take that copy of the standard with you if you leave one job for another. As in many other professions, so it is with auditing—knowledge is power.
- Don't be afraid to share or collaborate. I wrote an article that was published in *Quality Progress* providing a framework for objectively and consistently evaluating an internal audit program. I created the form in MS Word. One reader asked if he could

have permission to use the form, to which I replied "certainly, as long as you retain my copyright on the documents." The gentleman agreed and sent me a copy of the modified form that he had created for his organization's use based on my original template. He had converted my original Word file into an Excel spreadsheet with cells containing calculations, a second tab for notes, and a third for graphs, resulting in a format that both functioned better and was more visually appealing. He graciously allowed me to adopt his new and improved version for my own use. So by sharing and collaborating I arrived at an even more valuable tool to aid in the continuous improvement of my own audit program.

DESK AUDITS

A desk audit, also known as a *document audit*, is a review of an organization's documents by an auditor. It is one of the first audit steps taken to ensure that an adequate quality management system is maintained. It is referred to as a desk audit because it can be conducted at the auditor's desk since there is no requirement to walk the manufacturing floor or interview auditee employees. One benefit of a desk audit is that it guides the lead auditor in where to focus limited resources when conducting the on-site portion of the audit. It also provides information that helps in the preparation of more-detailed checklists and questionnaires. Another benefit of desk audits is that if it is determined during this documentation review that an adequate quality management system is not maintained, the audit can be terminated at that point and requests for corrective action may be submitted as appropriate. In such a case, conducting the desk audit would save the cost of travel for an on-site audit that would not have been successful. As we have just discussed, a desk audit can be conducted during the planning phase of an on-site audit. A desk audit can also be a stand-alone audit if risk indicates that, while an assessment of the quality management system is needed, the expense of an on-site audit is not warranted.

The key to successful desk audits is to request sufficient documentation to effectively assess the auditee's quality management system and to schedule adequate time for that review. Reviewing just the quality manual doesn't get it. There is not enough detail at that level of documentation. Following is a partial listing of some of the documents that might be requested as part of a desk audit:

- Quality manual

- Contract review
- Control of nonconforming material
- Corrective and preventive action
- Internal audits
- Receiving, in-process, and final inspection
- Customer property
- Complaint handling
- Customer returns
- Customer notification
- Identification and traceability
- Record retention
- Process monitoring and control
- Control of suppliers

Assessment of the quality management system during a desk audit is accomplished by review of the quality manual along with second-tier documents (for example, standard operating procedures) against external requirements (such as regulations and ISO standards) and against internal requirements (like quality agreements, purchase orders, and product specifications). Third-tier (work instructions, drawings, flowcharts, and so forth) and fourth-tier (records, forms, templates, and so on) documented information would typically be reviewed while on-site. Some of the things that an auditor is looking to verify during a desk audit are:

- All of the required documents are in place. If so, is all required information contained within?
- Required records are maintained; actual record review would be accomplished on-site (in some cases relevant records might be reviewed as part of a stand-alone desk audit).
- Related documents support and not contradict one another.
- Documents are clear and unambiguous.
- The supplier ISO and/or other relevant certifications are current.

- Identification of procedural gaps in meeting expectations of the auditing body or the application of standard practices to common processes (opportunities for improvement).

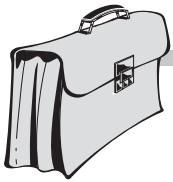
Something to be wary of is that there can sometimes be a tendency to make desk audits a "check-box" exercise if it is decided that there will not be an accompanying on-site audit. This is a big mistake! A properly conducted desk audit can take hours to complete—minimally between four and eight hours. It is not something to be scheduled to "knock out" over the course of a couple hours during one afternoon. A benefit of desk audits is that other work can be done while conducting the audit. With that being said, a desk audit could take place across several days or even a couple of weeks depending on how busy the auditor is. Thus, it is important to keep track of the audit status to ensure that audit completion doesn't fall through the cracks.

VIRTUAL AUDITS

Virtual audits are closer to on-site audits than desk audits in that they include real-time engagement with the auditee as documents and records are reviewed, such as using video or teleconferencing technology, as opposed to being face to face. Desk audits, on the other hand, are a combination of discrete actions as documents and records are requested and then reviewed off-line by the auditor. Then the auditor contacts the auditee with any questions to be answered and awaits a response. During the desk audit there is a lot of stop, go, and wait as the involved parties conduct the audit asynchronously. Just as a person can get a lot more information and be much clearer in a phone call than via e-mail, there is a similar advantage to virtual auditing over desk auditing. Another significant advantage is that with virtual auditing the auditor can witness and process nonverbal cues, which will help in their interpretation of audit findings. As with on-site audits, a desk audit might be a *part* of a virtual audit, as the auditor might want to review certain documents ahead of time in order to optimize the time spent "live" with the auditee. There is a risk in conducting virtual audits in lieu of on-site audits in that certain nonverbal cues may be missed and the auditor may draw incorrect conclusions. So, the benefits of performing virtual audits must be balanced against the risks.

Videoconferencing can range from using the Skype for Business application on your computer to having a $100,000 videoconferencing

center with multiple workstations, 72-inch monitors, and deluxe swivel seating. There are also many free and low-cost applications that allow for video-conferencing if budget is a significant issue. In a pinch, you could even use Apple's FaceTime if you had to. The key is that there has to be a matching system on each end of the conversation. The boundaries of real-time engagement through virtual auditing are only limited by the technology available to all parties. At one company, I witnessed a 13-inch monitor on a radio-controlled wheeled platform projecting the face of a manager that could speak with individuals in the area. The platform contained a camera that could see activities going on within the office and on the manufacturing floor. This happened to be within one facility, but imagine if you could use similar technology across sites or between companies! Both desk and virtual audits go through the same reporting and closure process as on-site audits.



CASE IN POINT

We May Have Become a Little Complacent: Or a Practical Application of Risk-Based Thinking

For an example of how to apply risk-based thinking to an audit, let's look at the following true scenario. Company ABC has a supplier XYZ just outside of San Francisco that has successfully produced a part for 20 years. At various times, they have outperformed competing suppliers. Per new supply chain guidelines, supplier XYZ was included on the year's audit schedule since they had never been audited previously. Everyone assumed that, based on past performance, the audit would go swimmingly. That's why I included them on *my* audit schedule. Alas, such was not to be the case.

As part of my preparation for conducting the audit, I made copies of the documentation packets for the last three shipments received prior to the audit date. It was my intent to perform a backward trace as part of the audit. The first step—after I had arrived, introduced myself, and been through the site tour—was to ask to see their documentation for the last three lots shipped. As expected, what they had in their files matched what I had in my hand. Check. Based on the fact that this was such a small shop, I began thinking to myself, "Hmmm, maybe I will even have time to stop by the wine country on my way out of town." Next, I asked to see the production records for the three lots in question, to which the auditee representative responded, "You have the records." I responded, "Are you saying that you

sent the milling, inspection, test, and other production records along with your certificates of conformance and analysis?" "Oh no, we didn't do that. Let me get you the production records." What they brought back was a six-by-six-inch square box jammed full of slips of paper. This didn't *seem* like a lot of production records, but I wasn't sure how they segmented their records and wasn't exactly sure what I was looking at. This wasn't an immediate concern since their production records were documented on six-by-nine-inch sheets of paper. So I asked, "Are the production records that I am looking for in this box?" "Well, no." This reminded me of a comedic sketch that I watched once where the comedian was getting frustrated because his partner didn't understand what he was asking and began saying to the "straight man," "*Do you understand the words that are coming out of my mouth*?"

At this point, I began to speak a little more slowly and loudly (as if this would help) as I repeated myself. What I would like to see . . . are the milling . . . inspection . . . test . . . and other production records . . . for these . . . three . . . lots. Pause. "Let me get the owner."

Owner: "So you want to see the production records for these three lots?"

LBC: "Yes, I do."

Owner: "You see we have been making these parts for a long time."

LBC: "Yes, you have. Almost 20 years."

Owner: "These kinds of records can take up a lot of space over the years."

LBC: "Yes, they might."

Owner: "Well, we may have become a little complacent over the years."

LBC: "Please tell me more."

Owner: "We decided last year to only keep the production records for the previous month's runs. We only keep the shipping certifications and other documents for longer than that."

LBC: "Okay. Well, what would happen if we notified you of a problem with a lot that you shipped more than a month ago and asked you to investigate what happened?"

Owner: "We wouldn't be able to."

LBC: "Well, you can see where I might be concerned with this practice, can you not?"

Owner: "Yes, of course. We have been producing these parts for so long that we have become complacent and made a bad decision."

LBC: "Thank you for your frankness in explaining your process. We will revisit this finding during the closing meeting."

Owner: "Of course."

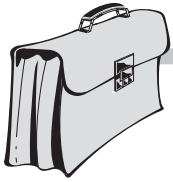
Next, I went into the metrology department and saw this really cool $10,000–plus laser micrometer! (I know, my inner geek is showing.) It was used to measure the diameter of the blank rods that would be milled and processed to eventually become our parts. While the area supervisor was demonstrating how to use the device, I noticed that the calibration sticker on the side said 2009. Did I mention that this audit took place in 2014? I'm now thinking, "Maybe I won't get to the wine country after all." When I inquired as to why the calibration sticker said 2009, the supervisor replied that they had it calibrated after the initial purchase in 2009. I then asked, "How do you protect from drift and ensure that the laser micrometer remains accurate after all of these years?" "Well, we check it daily across the full range of values using gage pins." Since this is an acceptable practice, I asked to see the gage block set that was used to calibrate the laser micrometer. He showed me, and I found the set to be completely well maintained and in a padded wooden box made to house the pins. However, when I flipped the box over and looked at every exterior and interior side, I had to ask, "Where is the calibration sticker for the gage pin set?" "Oh, those aren't calibrated." Starting to speak slowly, *again,* "Okay. So how do you know that these gage pins are accurate?" "We check them with the laser micrometer." (This time I paused . . . .)

My response: "Well, whatever standard that you use to calibrate a piece of equipment that is used to accept product has to be calibrated by a standard having traceability back to NIST (National Institute for Standards and Technology). So, you can use the gage pins to calibrate your laser micrometer as you have described, but those gage pins must themselves be calibrated." Pause. "Let me go get the owner."

When all was said and done, there were two nonconformities concerning calibration, one for the quality manual, and one for records maintenance (or lack thereof) raised during the audit. If this were a new supplier assessment, the supplier would have been rejected out of hand. However, Supplier XYZ has consistently had one of the best quality and on-time-delivery records. Now what to do? Apply risk-based thinking to the situation!

It is at this time when proper assessment of the level and type of risk is important. Because none of the nonconformities directly impacted product or product realization, and based on both recent and past history, the risk to product was deemed low. However, the risk to successful implementation of the QMS (the ability to monitor the effectiveness and efficiency of the company quality management system and determine root cause when something goes wrong) was high. In other words, despite Supplier XYZ's excellent historical production record, if something did go wrong in the future, the supplier's ability to detect and respond effectively could be negatively impacted by these findings.

All four findings were classified as major, and Supplier XYZ was downgraded from "approved" to "conditionally approved" status on the approved supplier list. From the perspective of Company ABC, orders could still be placed with XYZ as long as the findings were responded to with effective corrective action within a six-month window. So, other than a loss of face, no business harm would come to Supplier XYZ as long as they determined and implemented a robust corrective action plan. Also, rather than schedule the next audit for three years ahead, as would typically be the case, it was determined that a follow-up audit should be conducted the following year. These measures allowed Company ABC to take a firm stand in order to address future risk while still acknowledging the solid performance history of XYZ. Supplier XYZ did implement corrective actions as promised and passed a follow-up audit.



CASE IN POINT

Catfight: A Tale Showing the Pros and Woes of Virtual Auditing

By Shauna Wilson

Nonverbal communication between people is communication through sending and receiving wordless clues. It includes the use of visual cues, such as body language (kinesics), distance (proxemics), and physical environments/appearance of voice (paralanguage), and of touch (haptics). It is estimated up to 65 percent of communication is nonverbal; it has been said, "The most important thing in communication is to hear what isn't being said."

—Peter F. Drucker

Late one evening in an online meeting with a client in another part of the world, I was provided feedback on a recent internal audit conducted virtually. My findings included three different responses to a shared process. As I met virtually with three gentlemen who sat together in a conference room, I reported my findings to them using a collaborative program to illustrate the objective evidence. We used no cameras, thus, we could not see one another. English is my first language, but it wasn't theirs. I explained my findings and asked a simple question—which process is correct? There was a long silence, and then suddenly an argument broke out. Exacerbated by the sound of a different language and the speed with which they were spewing their words, from my end it sounded like a catfight. As they argued, I thought, "Would they have behaved this way if I was there in the conference room or if we had cameras on?" As suddenly as the argument started, it stopped. All was quiet! Breaking the silence, I asked them for their decision, and the manager responded in English with the process to be used.

> *An eAudit is a systematic, independent, and documented process to obtain evidence through electronic means to determine the extent of conformity to the audit criteria.*
>
> —J.P. Russell

In this story an interstate and international internal audit conducted virtually found process failures and communication issues between entities located in three countries. An advantage eAuditing offers over face-to-face (FtF) auditing is the ability to conduct a whole system review of the global supply chain with the same auditor connecting the distal processes together. This finding might have been missed if conducted in a traditional FtF audit with limited locational boundaries and multiple local auditors. An eAudit or virtual audit uses the same audit process as an FtF audit except for conducting the audit through electronic means at remote locations. Unlike a desk audit, eAudits are simultaneous, where the auditor and the auditee are present in their remote locations, viewing documents or processes simultaneously over collaborative programs. Virtual teams have communicated and worked together online for 20 years, but the use of auditing virtually or eAuditing is still not an accepted audit method by most registrars. Many report that European registrars will not accept internal audits that are conducted virtually. Stated validation concerns include the ease of hiding things from auditors and limited nonverbal communication. Admittedly, the auditor conducting eAudits will need more skills in technology and communication methods, and knowledge of cultural differences, to be successful.

For instance, auditors need to understand communication methods, including how to replace nonverbal communication and mediate self-monitoring behavior. Nonverbal communication includes facial expressions and body language often used in FtF communication. Self-monitoring behavior is focused on changes in an individual's behavior when not meeting FtF. Self-monitoring behavior is rated in terms of high or low behavior. Simply put, people with low self-monitoring behavior do not self-govern their behavior when they are not physically present; behavior can include tardiness, rude comments, and reading e-mails or texting during a virtual meeting. High self-monitoring people do not have to be watched; they are able to keep the same standards of politeness and respect in both FtF and virtual environments.

Reliance on nonverbal communication is a primary method of communication in most cultures. The lack of nonverbal communication can be a barrier at times when cameras are limited. Audible nonverbal cues, like voice tone changes or a delayed response, can become an indicator to ask more questions on a subject. But, in this story, it was not the nonverbal communication that exposed miscommunication between the entities. It was preparation and skillful auditing, asking thoughtful questions, and following audit trails and objective evidence that discovered the process failure. In a way, eAuditing may move auditors to depend less on nonverbal communication and focus more on the audit and communication processes and research methods to find objective evidence. Cameras may help to manage low self-monitoring behavior but will not completely replace all aspects of FtF nonverbal communication. In the story, would cameras have prevented the outburst or been forgotten like the microphone, which could have been muted during their conversation?

The argument was the result of a miscommunication; either we did not communicate that correctly, or the communication was taken out of context and misinterpreted. Communication is blamed for most things that go wrong in our personal and business lives. Yet, most people are unaware of communication processes that will help others to understand information. A communication process commonly used for laying the groundwork for a conversation is the three-stage communication development approach. The initial stage focuses on *background research* on a subject matter, person, or event. For example, many people instantly Google or ask friends about topics before going to an interview. The second stage is a *discussion* phase with the person after the initial research, where people will talk about commonalities to build trust. An important aspect of the second stage is the decision to make collaborative plans and continue to stage three. People

can decide not to continue to stage three if they are not committed to work toward the same goal. In stage three, people *jointly lay a path to work together*, those in new relationships will meet regularly, and teams begin new processes. In audits the three-stage communication approach can be applied to the audit process, as shown in Figure 2.9.

In preparing for the audit's closing meeting, I used the three-stage communication model to outline communication steps and address potential variables related to nonverbal communication, self-monitoring behavior aspects, and technology. Table 2.1 outlines the stages associating related variables.

I had assumed a miscommunication issue between all parties as the root cause. What I did not understand was the foundational process that needed to be followed. During initial research (stage one), I met with senior management, with whom I shared my finding and from whom I received information regarding the foundational standard process. The manager's feedback gave me information clarifying why the processes were not aligning. Learning these details, the closing meeting (stage two) needed to illustrate to the three members the objective evidence and its overall result of divergent processes. To remove blame, the results had to be clear and visual in order to impart an understanding to mitigate any low self-monitoring behavior. Because of the distance over which the party met together, I decided that respectfulness should stay within cultural norms, even with their culturally competitive nature. In the end, the team members worked together to follow the foundational process. Culture plays a very big role in global supply chain audits. I believe the response was mostly cultural; low self-monitoring behavior may have resulted in someone leaving the meeting or stating agreement without follow-through.

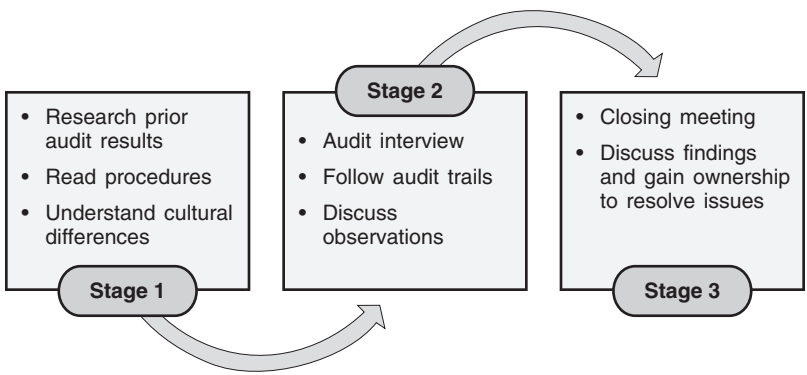


Figure 2.9 Three-stage communication development process.

An overlooked aid to eAudits may be the newly released ISO 9001:2015 standard and the requirement to understand the context of the organization. The new standard leads us to understand just how complex businesses have

Table 2.1 Three-stage communications model.

Three-stage communication development stages	Potential communication variables	
	Nonverbal communication	**Self-modification behavior**
Stage 1 Passive social information-seeking prior to speaking to others; assess working environment and gather background information	Understand: • Nonverbal communication indicators within a cultural sense • No cameras or visual appearance for the auditor – Only audio • Auditees are meeting FtF, the auditor is remote	Seek knowledge on cultural differences: • The response to feedback or critique • Competitive work environment • Competitive culture
Stage 2 People discuss experience, find commonality, and share process issues	Replace nonverbal communication with: • Clear display of the audit findings • Clear statement of discovered process gaps • Remove the personal and location reference	Prepare for: • Auditees meeting FtF; self-monitoring behavior at remote site should be high; face saving should be active • Response will be cultural and the nature of the work environment highly competitive
Stage 3 People decide to either make plans or not become involved in the solution	• The discussion at the remote location gave an impression they were fighting. It was unintelligible due to language differences, but the reaction is considered cultural	• No one left the room • Each team member committed to improvement plans and followed through to resolve issues

become by competing in a global market. When the context of the business is understood and interested parties are identified, risk-based thinking tools could include a hybrid auditing model for understanding quality system performance. A hybrid auditing model may include multiple methods like eAudits, FtF and desk audits, supplier reviews or regular yield reporting, random third-party product testing, and customer surveillance audits (auditors posing as customers).

eAuditing in a hybrid model is an efficient and effective audit method optimizing the use of limited resources. The following activities can leverage eAuditing methods:

- Visual verification at an external provider's location to understand process-related issues
- Reviewing product-related issues in real time at a remote location, or verifying that a change has been implemented
- Enhancing understanding among interested parties because everyone can see document content or processes simultaneously

Companies that invest in eAuditing allow remote locations to learn from one another as they gain a better understanding of remote processes, and leverage and standardize common processes. Rather than refusing eAuditing methods, prioritize to invest in the technology training. Practicing online facilitation, learning new skills to replace nonverbal communication, and engaging in intercultural studies should be at the forefront of both internal and external auditors' professional goals.

Shauna Wilson, *President at Amazon Consulting Inc., is a performance management consultant designing efficient and effective quality systems. Shauna is an IRCA-certified auditor and leading expert in remote auditing. She holds an MS in performance management technologies/instructional design. Shauna wrote* InterneTeaming.com: Tools to Create High Performance Remote Teams *and coauthored* eAuditing Fundamentals: Virtual Communication and Remote Auditing, *and was featured in* Quality Progress, The Auditor, *and ASTD's* InfoLine. *Shauna is the Education/Social Responsibility Chair at 607 Portland ASQ Section and currently serves as the USTAG Expert for PC/TAG302 ISO19011 Auditing Management Systems.*

Appendix

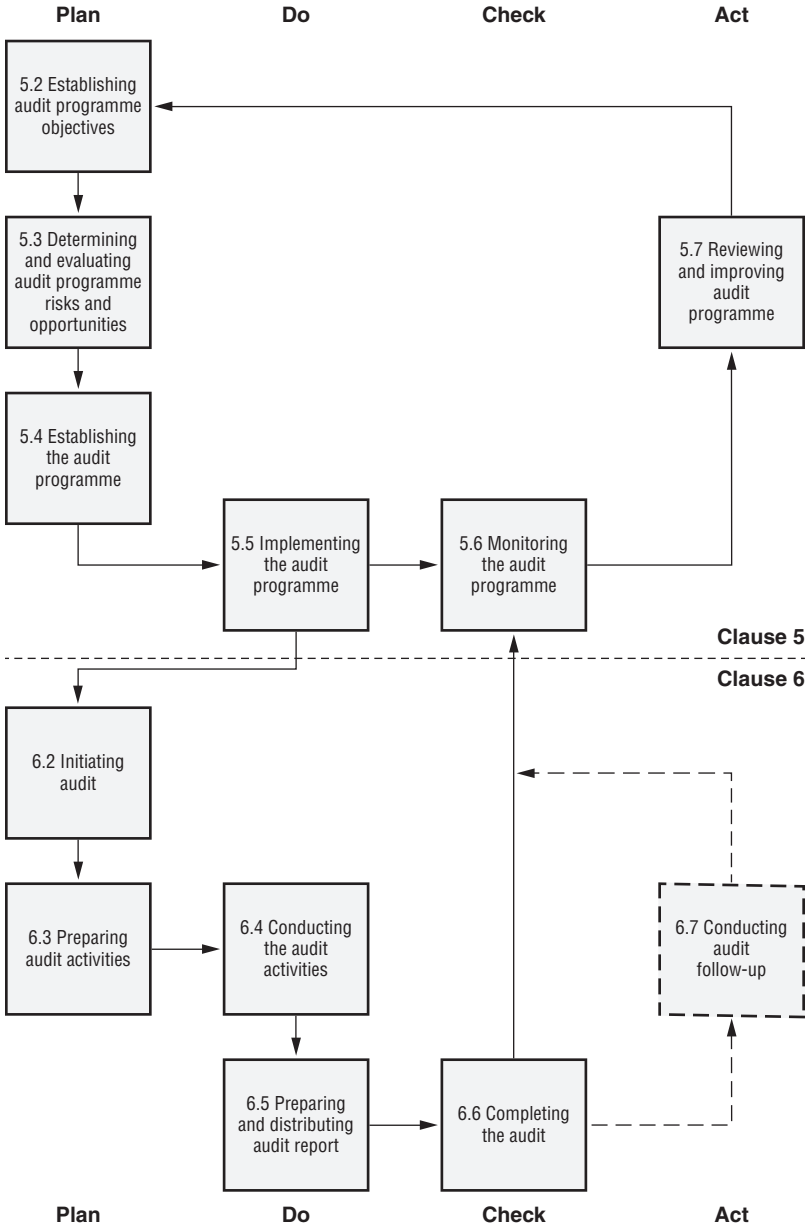
ISO 19011:2018 User's Guide

ISO 19011:2018 *Guidelines for auditing management systems* provides the foundation for best auditing practices worldwide. Several hundred auditors, many with decades of auditing and quality management experience, came together from around the globe over the course of two years to contribute to the latest version of this standard. ISO 19011 is important because it forms the basis of auditing techniques for many certifications, such as the ASQ Certified Quality Auditor and Exemplar Global (as well as other auditor certifying bodies) Lead QMS Auditor certifications.

Most auditor certifications are a combination of bodies of knowledge—auditing tools and methods plus some additional ones. For industry-specific certifications, industry-specific requirements (whether regulatory or ISO or both) would be combined with auditing tools and techniques. For the ASQ Certified Quality Auditor designation, meant to allow auditors to audit successfully across multiple industries, auditing tools and techniques are combined with an in-depth study of quality tools, risk management, lean and Six Sigma, basic statistics, and so forth. In both of these cases, the methodology for employing auditing tools and techniques comes from ISO 19011.

The standard is well thought-out and provides its own "Cliff's Notes" for auditors who just want to use it as a quick reference guide. The content of ISO 19011:2018 is summarized in two process flow diagrams found in Figures 1 and 2 within the standard (see Figures A.1 and A.2). The top half of Figure 1 represents clause 5 and shows how an organization goes about establishing audit program guidelines, while the bottom half representing clause 6 shows the next level down, how to conduct an audit. Finally, Figure 2 provides detail on how to collect and verify evidence while conducting the audit. Figure 1 references the paragraphs within the standard where the reader can get further detail.

One significant change to the 2018 edition of the standard is a more in-depth discussion of addressing risks and opportunities for both the audit



Note 1: This figure illustrates the application of the Plan–Do–Check–Act cycle in this document.

Note 2: Clause/subclause numbering refers to the relevant clauses/subclauses of this document.

Figure A.1 Process flow for the management of an audit program.

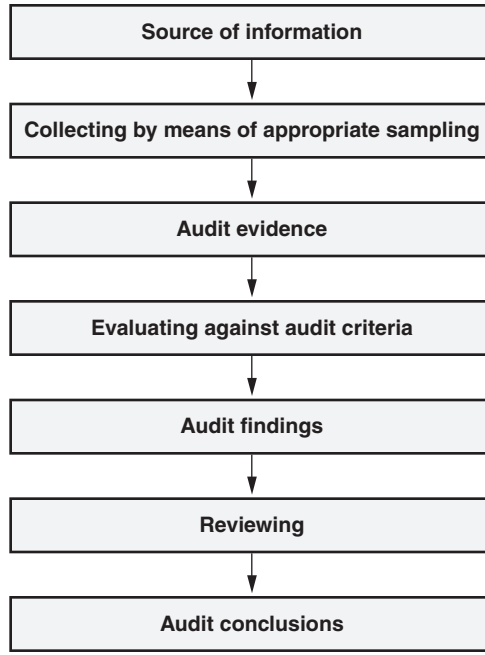


Figure A.2 Overview of the process of collecting and verifying information.

program and the quality management system that it is meant to monitor. As expected, there is the addition of the risk-based approach to the principles of auditing. Also, expansion of the guidance on managing an audit program, including audit program risk. New technologies are addressed as in the discussion on virtual auditing found in the annexes, which provide additional guidance for auditors regarding key topics. There are also updated requirements relating to audit plans, which are addressed as the output of the audit planning process.

ISO 19011 starts with scope, normative references, and terms and conditions, just like the related management system standards that this standard explains how to audit. After that, however, the section topics diverge to address the specifics of auditing as follows:

- Section 4 Principles of auditing
- Section 5 Managing an audit program
- Section 6 Conducting the audit
- Section 7 Competence and evaluation of auditors

- Annex A Additional guidance for auditors for planning and conducting audits

To recap, ISO 19011 provides a guideline for best auditing practices worldwide and is the foundation of most internationally recognized certified quality auditor bodies of knowledge. It can be used as a stand-alone auditor training manual or as a quick reference guide for experienced auditors, and is a worthwhile document for anyone interested in auditing to have in their library.

Glossary

audit—(1) Results of the evaluation of the collected audit evidence against audit criteria; (2) A systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.

consumer risk—The risk of accepting something bad as good.

element method—The auditor examines each element of a standard or regulation to see how effectively it is implemented within the entire system.

hazard—Something found in the environment that is a potential source of harm, and that has a risk attached; typically a noun. For example, an extension cord stretched across a walkway would be a hazard. The risk attached would be that of tripping and falling. The harm would be the injury that might come from the fall.

process approach—The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, to produce a desired outcome.

producer risk—The risk of rejecting something good as bad

risk—The effects of uncertainty (on results).

risk-based thinking—A process that evaluates data inputs from the perspective of risk, with the output being a risk management program or model.

risk management—Coordinated activities to direct and control an organization with regard to risk.

risk tolerance—How willing a company is to accept risk in order to achieve a perceived benefit.

sole source—The only supplier from which you can acquire a particular product.

single source—Whereas there may be multiple places to acquire a particular product, this is the only supplier that has been qualified to provide it to you. Thus, replacement of this supplier could be costly in both time and expense.

supplier audit—On-site (supplier) verification activity, such as inspection or examination, of a process or quality system to ensure compliance to requirements.

supply chain—The global network used to deliver products and services—from raw materials to end customers—through an engineered flow of information, physical distribution, and cash.

supply chain management—The design, planning, execution, *control*, and *monitoring* of supply chain activities with the objective of creating net value, building a competitive infrastructure, leveraging worldwide logistics, synchronizing supply with demand, and measuring performance globally.

Bibliography

APICS. 2016. *Basics of Supply Chain Management: Participant Workbook*. Chicago: APICS.

Blanchard, Ken, and Jesse Lyn Stoner. 2011. *Full Steam Ahead! Unleash the Power of Vision in Your Work and Your Life*. San Francisco: Berrett-Koehler.

Durivage, Mark Allen. 2017. *The Certified Supplier Quality Professional Handbook*. Milwaukee: ASQ Quality Press.

Myerson, Paul. 2012. *Lean Supply Chain and Logistics Management*. New York: McGraw Hill.

Okes, Duke. 2013. *Performance Metrics: The Levers for Process Management*. Milwaukee: ASQ Quality Press.

Russell, J.P., editor. 2013. *The ASQ Auditing Handbook*. 4th ed. Milwaukee: ASQ Quality Press.

Russell, J.P., and Shauna Wilson. *eAuditing Fundamentals: Virtual Communication and Remote Auditing*. Milwaukee: ASQ Quality Press.

(This page intentionally left blank)

Index

J

K

L

M

N

O

P

R

S

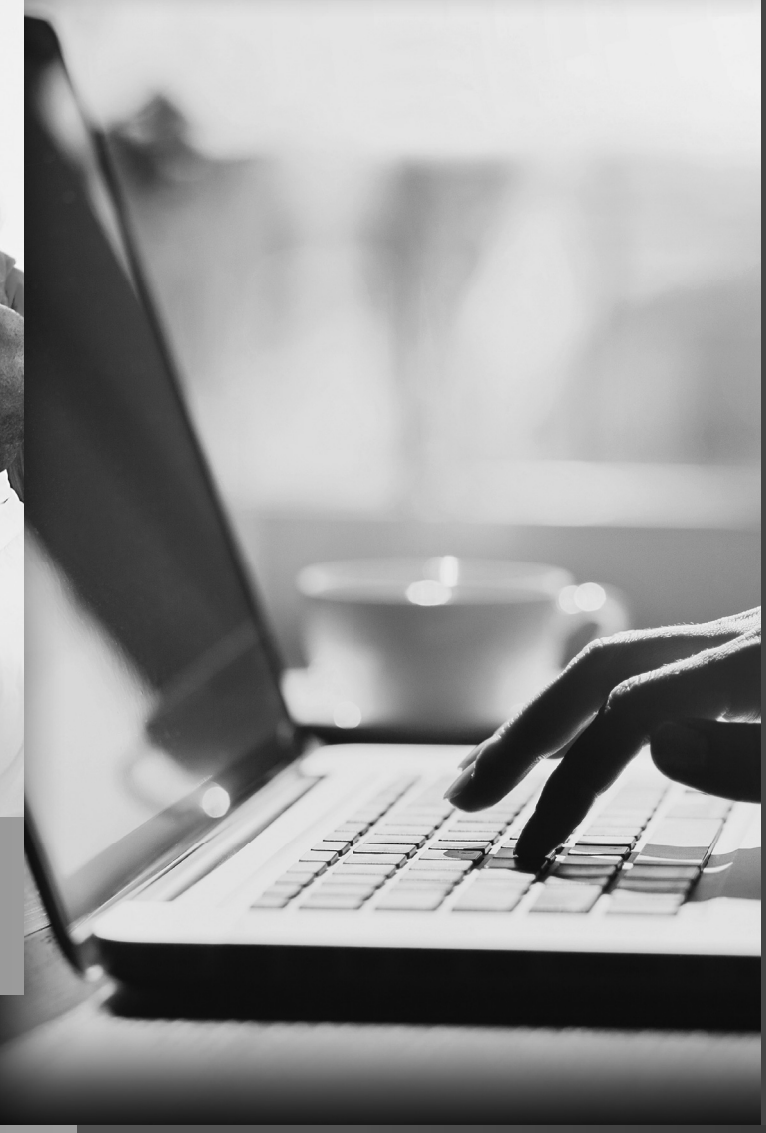
T

V

W

Z


WHY ASQ?
ASQ is a global community of people passionate about quality, who use the tools, their ideas and expertise to make our world work better. ASQ: The Global Voice of Quality.
FOR INDIVIDUALS
Advance your career to the next level of excellence.
ASQ offers you access to the tools, techniques and insights that can help distinguish an ordinary career from an extraordinary one.
FOR ORGANIZATIONS
Your culture of quality begins here.
ASQ organizational membership provides the invaluable resources you need to concentrate on product, service and experiential quality and continuous improvement for powerful top-line and bottom-line results.
www.asq.org/why-asq
ASQ
The Global Voice of Quality®



ASQ'S ONLINE QUALITY RESOURCES IS THE PLACE TO:

- Stay on top of the latest in quality with Editor's Pick and Most Popular
- Browse topics in Learn About Quality
- Find definitions in the Quality Glossary
- Search ASQ's collection of articles, books, tools, training, and more

QUALITY RESOURCES
www.asq.org/quality-resources

Connect with ASQ staff for personalized help hunting down the knowledge you need, the networking opportunities that will keep your career and organization moving forward, and the publishing opportunities that offer the best fit for you.

www.asq.org/quality-resources

ASQ
The Global Voice of Quality®

TRAINING CERTIFICATION CONFERENCES MEMBERSHIP PUBLICATIONS

ASK A LIBRARIAN

Have questions? Looking for answers? In need of information? Ask a librarian!

Customized research assistance from ASQ's research librarian is one of the many benefits of membership. ASQ's research librarian is available to answer your research requests using the everexpanding library of current and credible resources, including journals, conference proceedings, case studies, and Quality Press publications.

You can also contact the librarian to request permission to reuse or reprint ASQ copyrighted material, such as ASQ journal articles and Quality Press book excerpts.

For more information or to submit a question, visit asq.org/quality-resources/ask-a-librarian.

ASQ
The Global Voice of Quality®

TRAINING CERTIFICATION CONFERENCES MEMBERSHIP PUBLICATIONS